PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-344444
(43)Date of publication of application : 29.11.2002

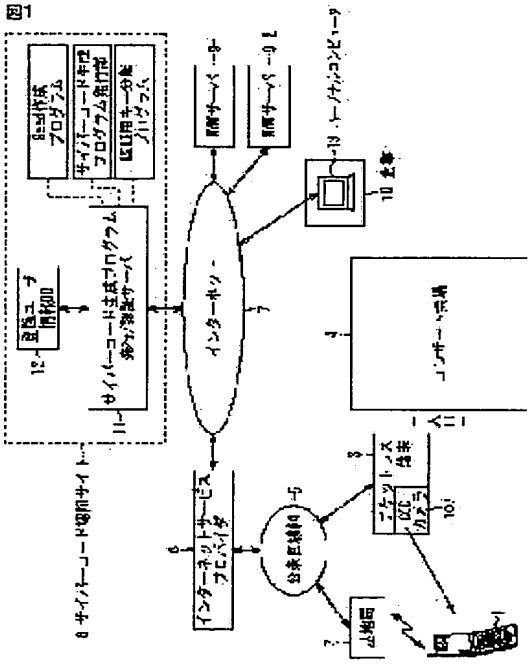
(51)Int.Cl. H04L 9/32
G06F 12/14
G06F 15/00
G06F 17/60

(21)Application number : 2001-148576
(22)Date of filing : 18.05.2001

(71)Applicant : SONY CORP
(72)Inventor : FUKUDA JUNKO
IHARA KEIGO
SUEYOSHI TAKAHIKO
AYATSUKA YUJI
MATSUSHITA NOBUYUKI
REKIMOTO JIYUNICHI

(54) INFORMATION PROVIDING DEVICE AND METHOD, INFORMATION PROCESSING DEVICE AND METHOD, INFORMATION AUTHENTICATING DEVICE AND METHOD, AUTHENTICATING SYSTEM, RECORDING MEDIUM AND PROGRAM OF THEM

(57)Abstract:
PROBLEM TO BE SOLVED: To make a program itself function as an authentication key.
SOLUTION: A cyber-code authenting site 8 prepares a cyber-code generation program based on a user ID, a random number, and the present time, and transmits it to a portable telephone set 1. The portable telephone set 1 executes the received cyber code generation program, and generates and displays a cyber code. A ticketless terminal 3 images the cyber-code displayed at the portable telephone set 1 by a CCD camera 107, and transmits the recognized code number to a cyber-code authentication site 8. The code-code authentication site 8 retrieves the random number and the time information from a registered user information DB 12, based on the user ID included in the code number, and prepares the cyber-code generation program gain. Then, the user is authenticated from the code number of the cyber-code obtained by executing the prepared program.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

THIS PAGE LEFT BLANK

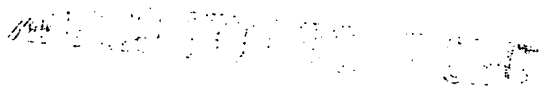
[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]



THIS PAGE LEFT BLANK

(19)日本国特許庁(JP)　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開２００２－３４４４４４
（Ｐ２００２－３４４４４４Ａ）
(43)公開日　平成14年11月29日(2002.11.29)

(51)Int.Cl.⁷		識別記号	FI			テーマコード(参考)
Ｈ０４Ｌ	9/32		Ｇ０６Ｆ	12/14	３２０Ｆ	5B017
Ｇ０６Ｆ	12/14	３２０		15/00	３３０Ａ	5B085
	15/00	３３０		17/60	１４０	5J104
	17/60	１４０			１４６Ａ	
		１４６			５０６	

審査請求　未請求　請求項の数２４　ＯＬ　（全２９頁）　最終頁に続く

(21)出願番号　特願2001-148576(P2001-148576)

(22)出願日　平成13年5月18日(2001.5.18)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川6丁目7番35号

(72)発明者　福田　純子
東京都品川区北品川6丁目7番35号　ソニー株式会社内

(72)発明者　井原　圭吾
東京都品川区北品川6丁目7番35号　ソニー株式会社内

(74)代理人　100082131
弁理士　稲本　義雄

最終頁に続く

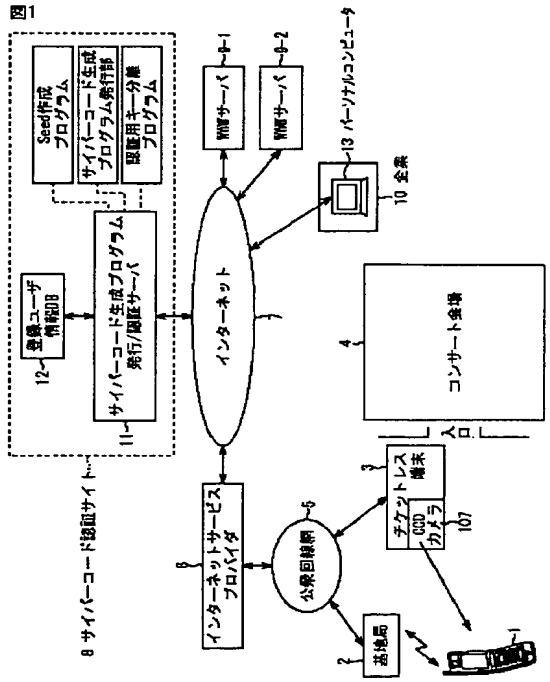
(54)【発明の名称】情報提供装置および方法、情報処理装置および方法、情報認証装置および方法、認証システム、記録媒体、並びにプログラム

(57)【要約】

【課題】　プログラム自体を認証キーとして機能させるようにする。

【解決手段】　サイバーコード認証サイト８は、ユーザID、乱数および現在時刻を基に、サイバーコード生成プログラムを作成し、携帯電話機１に送信する。携帯電話機１は、受信したサイバーコード生成プログラムを実行してサイバーコードを生成し、表示させる。チケットレス端末３は、携帯電話機１に表示されているサイバーコードをCCDカメラ１０７で撮像し、認識されたコード番号をサイバーコード認証サイト８に送信する。サイバーコード認証サイト８は、コード番号に含まれるユーザIDを基に、登録ユーザ情報DB１２から乱数および時刻情報を検索し、再度サイバーコード生成プログラムを作成する。そして、作成されたプログラムを実行することにより得られるサイバーコードのコード番号から、ユーザが認証される。

図1



1

【特許請求の範囲】

【請求項１】　情報処理装置から送信されてくるプログラムの発行要求を受けて、前記情報処理装置に対して、ユーザIDを発行する発行手段と、
前記発行手段により発行された前記ユーザID、および前記発行要求の受信時刻を基に、乱数を発生する乱数発生手段と、
前記乱数発生手段により発生された前記乱数、前記ユーザID、および前記受信時刻を基に、所定画像を生成するための前記プログラムを作成する作成手段と、前記作成手段により作成された前記プログラムを前記情報処理装置に提供する提供手段とを備えることを特徴とする情報提供装置。

【請求項２】　前記ユーザIDに対応付けて、前記乱数および前記受信時刻を記録する記録手段をさらに備えることを特徴とする請求項１に記載の情報提供装置。

【請求項３】　前記所定画像は、２次元コードであることを特徴とする請求項１に記載の情報提供装置。

【請求項４】　情報処理装置から送信されてくるプログラムの発行要求を受けて、前記情報処理装置に対して、ユーザIDを発行する発行処理ステップと、
前記発行処理ステップの処理により発行された前記ユーザID、および前記発行要求の受信時刻を基に、乱数を発生する乱数発生処理ステップと、
前記乱数発生処理ステップの処理により発生された前記乱数、前記ユーザID、および前記受信時刻を基に、所定画像を生成するための前記プログラムを作成する作成処理ステップと、
前記作成処理ステップの処理により作成された前記プログラムを前記情報処理装置に提供する提供処理ステップとを含むことを特徴とする情報提供方法。

【請求項５】　情報処理装置から送信されてくるプログラムの発行要求を受けて、前記情報処理装置に対して、ユーザIDを発行する発行処理ステップと、
前記発行処理ステップの処理により発行された前記ユーザID、および前記発行要求の受信時刻を基に、乱数を発生する乱数発生処理ステップと、
前記乱数発生処理ステップの処理により発生された前記乱数、前記ユーザID、および前記受信時刻を基に、所定画像を生成するための前記プログラムを作成する作成処理ステップと、
前記作成処理ステップの処理により作成された前記プログラムを前記情報処理装置に提供する提供処理ステップとを含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【請求項６】　情報処理装置から送信されてくるプログラムの発行要求を受けて、前記情報処理装置に対して、ユーザIDを発行する発行処理ステップと、
前記発行処理ステップの処理により発行された前記ユーザID、および前記発行要求の受信時刻を基に、乱数を発

2

生する乱数発生処理ステップと、
前記乱数発生処理ステップの処理により発生された前記乱数、前記ユーザID、および前記受信時刻を基に、所定画像を生成するための前記プログラムを作成する作成処理ステップと、
前記作成処理ステップの処理により作成された前記プログラムを前記情報処理装置に提供する提供処理ステップとをコンピュータに実行させるプログラム。

【請求項７】　情報提供装置から提供されるプログラムを取得する情報処理装置において、
前記情報提供装置に対して前記プログラムの送信を要求する要求手段と、
前記要求手段に基づいて前記情報提供装置から提供される前記プログラムを受信する受信手段と、
前記受信手段により受信された前記プログラムを実行し、所定画像を生成する生成手段と、
前記生成手段により生成された前記所定画像を表示する表示手段とを備えることを特徴とする情報処理装置。

【請求項８】　前記生成手段は、前記プログラムの実行時刻を基に、前記所定画像を生成することを特徴とする請求項７に記載の情報処理装置。

【請求項９】　前記生成手段は、所定時間毎に前記所定画像を生成し、
前記表示手段は、前記生成手段により所定時間毎に生成される前記所定画像を表示することを特徴とする請求項７に記載の情報処理装置。

【請求項１０】　前記所定画像は、２次元コードであり、
前記２次元コードには、ユーザIDを示すコード情報が含まれていることを特徴とする請求項７に記載の情報処理装置。

【請求項１１】　情報提供装置から提供されるプログラムを取得する情報処理装置の情報処理方法において、
前記情報提供装置に対して前記プログラムの送信を要求する要求処理ステップと、
前記要求処理ステップの処理に基づいて前記情報提供装置から提供される前記プログラムを受信する受信処理ステップと、
前記受信処理ステップの処理により受信された前記プログラムを実行し、所定画像を生成する生成処理ステップと、
前記生成処理ステップの処理により生成された前記所定画像を表示する表示処理ステップとを含むことを特徴とする情報処理方法。

【請求項１２】　情報提供装置から提供されるプログラムを取得する情報処理装置を制御するプログラムであって、
前記情報提供装置に対して前記プログラムの送信を要求する要求処理ステップと、
前記要求処理ステップの処理に基づいて前記情報提供装

置から提供される前記プログラムを受信する受信処理ステップと、
前記受信処理ステップの処理により受信された前記プログラムを実行し、所定画像を生成する生成処理ステップと、
前記生成処理ステップの処理により生成された前記所定画像を表示する表示処理ステップとを含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【請求項１３】　情報提供装置から提供されるプログラムを取得する情報処理装置を制御するコンピュータに、
前記情報提供装置に対して前記プログラムの送信を要求する要求処理ステップと、
前記要求処理ステップの処理に基づいて前記情報提供装置から提供される前記プログラムを受信する受信処理ステップと、
前記受信処理ステップの処理により受信された前記プログラムを実行し、所定画像を生成する生成処理ステップと、
前記生成処理ステップの処理により生成された前記所定画像を表示する表示処理ステップとを実行させるプログラム。

【請求項１４】　他の装置に記録されているユーザ情報を取得することが可能な情報認証装置において、
第１の画像を撮像する撮像手段と、
前記撮像手段により撮像された前記第１の画像に対応する第１の情報を認識する認識手段と、
前記認識手段により認識された前記第１の情報に含まれるユーザIDを基に、前記他の装置に記録されている前記ユーザ情報を検索する検索手段と、
前記検索手段により検索された前記ユーザ情報を基に、第２の画像を生成するためのプログラムを作成する作成手段と、
前記作成手段により作成された前記プログラムを実行し、前記第２の画像を生成する生成手段と、
前記生成手段により生成された前記第２の画像に対応する第２の情報と、前記認識手段により認識された前記第１の情報を認証する認証手段とを備えることを特徴とする情報認証装置。

【請求項１５】　前記撮像手段は、情報処理装置の表示部に表示されている前記第１の画像を撮像することを特徴とする請求項１４に記載の情報認証装置。

【請求項１６】　前記ユーザ情報は、少なくとも乱数および時刻情報を含み、
前記検索手段は、前記ユーザIDを基に、前記乱数および前記時刻情報を検索し、
前記作成手段は、前記検索手段により検索された前記乱数および前記時刻情報、並びに前記ユーザIDを基に、前記第２の画像を生成するための前記プログラムを作成することを特徴とする請求項１４に記載の情報認証装置。

【請求項１７】　前記生成手段は、前記プログラムの実行時刻を基に、前記第２の画像を生成することを特徴とする請求項１４に記載の情報認証装置。

【請求項１８】　前記第１の画像および前記第２の画像は、２次元コードであり、
前記第１の情報および前記第２の情報は、コード番号を示す情報であることを特徴とする請求項１４に記載の情報認証装置。

【請求項１９】　他の装置に記録されているユーザ情報を取得することが可能な情報認証装置の情報認証方法において、
第１の画像を撮像する撮像処理ステップと、
前記撮像処理ステップの処理により撮像された前記第１の画像に対応する第１の情報を認識する認識処理ステップと、
前記認識処理ステップの処理により認識された前記第１の情報に含まれるユーザIDを基に、前記他の装置に記録されている前記ユーザ情報を検索する検索処理ステップと、
前記検索処理ステップの処理により検索された前記ユーザ情報を基に、第２の画像を生成するためのプログラムを作成する作成処理ステップと、
前記作成処理ステップの処理により作成された前記プログラムを実行し、前記第２の画像を生成する生成処理ステップと、
前記生成処理ステップの処理により生成された前記第２の画像に対応する第２の情報と、前記認識処理ステップの処理により認識された前記第１の情報を認証する認証処理ステップとを含むことを特徴とする情報認証方法。

【請求項２０】　他の装置に記録されているユーザ情報を取得することが可能な情報認証装置を制御するプログラムであって、
第１の画像を撮像する撮像処理ステップと、
前記撮像処理ステップの処理により撮像された前記第１の画像に対応する第１の情報を認識する認識処理ステップと、
前記認識処理ステップの処理により認識された前記第１の情報に含まれるユーザIDを基に、前記他の装置に記録されている前記ユーザ情報を検索する検索処理ステップと、
前記検索処理ステップの処理により検索された前記ユーザ情報を基に、第２の画像を生成するためのプログラムを作成する作成処理ステップと、
前記作成処理ステップの処理により作成された前記プログラムを実行し、前記第２の画像を生成する生成処理ステップと、
前記生成処理ステップの処理により生成された前記第２の画像に対応する第２の情報と、前記認識処理ステップの処理により認識された前記第１の情報を認証する認証処理ステップとを含むことを特徴とするコンピュータが

読み取り可能なプログラムが記録されている記録媒体。

【請求項２１】　他の装置に記録されているユーザ情報を取得することが可能な情報認証装置を制御するコンピュータに、

第１の画像を撮像する撮像処理ステップと、

前記撮像処理ステップの処理により撮像された前記第１の画像に対応する第１の情報を認識する認識処理ステップと、

前記認識処理ステップの処理により認識された前記第１の情報に含まれるユーザIDを基に、前記他の装置に記録されている前記ユーザ情報を検索する検索処理ステップと、

前記検索処理ステップの処理により検索された前記ユーザ情報を基に、第２の画像を生成するためのプログラムを作成する作成処理ステップと、

前記作成処理ステップの処理により作成された前記プログラムを実行し、前記第２の画像を生成する生成処理ステップと、

前記生成処理ステップの処理により生成された前記第２の画像に対応する第２の情報と、前記認識処理ステップの処理により認識された前記第１の情報を認証する認証処理ステップとを実行させるプログラム。

【請求項２２】　情報提供装置、情報処理装置および情報認証装置からなる認証システムにおいて、

前記情報提供装置は、

前記情報処理装置から送信されてくるプログラムの発行要求を受けて、前記情報処理装置に対して、ユーザIDを発行する発行手段と、

前記発行手段により発行された前記ユーザID、および前記発行要求の受信時刻を基に、乱数を発生する乱数発生手段と、

前記乱数発生手段により発生された前記乱数、前記ユーザID、および前記受信時刻を基に、第１の画像を生成するための第１のプログラムを作成する第１の作成手段と、

前記第１の作成手段により作成された前記第１のプログラムを前記情報処理装置に提供する提供手段と、

前記ユーザIDに対応付けて、前記乱数および前記受信時刻を記録する記録手段とを備え、

前記情報処理装置は、

前記情報提供装置に対して前記第１のプログラムの送信を要求する要求手段と、

前記情報提供装置から提供される前記第１のプログラムを受信する受信手段と、

前記受信手段により受信された前記第１のプログラムを実行し、前記第１の画像を生成する第１の生成手段と、

前記第１の生成手段により生成された前記第１の画像を表示する表示手段とを備え、

前記情報認証装置は、

前記情報処理装置の前記表示手段に表示されている前記第１の画像を撮像する撮像手段と、

前記撮像手段により撮像された前記第１の画像に対応する第１の情報を認識する認識手段と、

前記認識手段により認識された前記第１の情報に含まれる前記ユーザIDを基に、前記情報提供装置の前記記録手段に記録されている前記乱数および前記受信時刻を検索する検索手段と、

前記検索手段により検索された前記乱数および前記受信時刻を基に、第２の画像を生成するための第２のプログラムを作成する第２の作成手段と、

前記第２の作成手段により作成された前記第２のプログラムを実行し、前記第２の画像を生成する第２の生成手段と、

前記第２の生成手段により生成された前記第２の画像に対応する第２の情報と、前記認識手段により認識された前記第１の情報を認証する認証手段とを備えることを特徴とする認証システム。

【請求項２３】　前記第１の生成手段は、前記第１のプログラムの実行時刻を基に、前記第１の画像を生成し、前記第２の生成手段は、前記第２のプログラムの実行時刻を基に、前記第２の画像を生成することを特徴とする請求項２２に記載の認証システム。

【請求項２４】　前記第１の画像および前記第２の画像は、２次元コードであることを特徴とする請求項２２に記載の認証システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、情報提供装置および方法、情報処理装置および方法、情報認証装置および方法、認証システム、記録媒体、並びにプログラムに関し、特に、２次元コードを生成するためのプログラムを認証キーとして利用するようにした情報提供装置および方法、情報処理装置および方法、情報認証装置および方法、認証システム、記録媒体、並びにプログラムに関する。

【０００２】

【従来の技術】従来から、物品の種類や状態などを示す英数文字をバーコード化し、例えば、物品に添付しておき、その添付されたバーコードを読み取って、物品の種類や状態などの情報を取得するバーコードシステムが、多くの産業分野に普及している。

【０００３】このようなバーコードは１次元バーコードと呼ばれ、太さの異なるバー（黒色の棒状部分）とスペース（空白部分）の組み合わせで所定のコードが示され、このコードパターンから読み出されるコード番号に基づいて、物品を識別し管理するようになされている。

【０００４】また、より多くの情報量をコード化するために、複数の方形セルを所定の配列規則に従って２次元的に配置させるような２次元コードも提案されている。２次元コードのコードパターンから読み出されるコード

番号は、固有（唯一）の番号であるため、特定のユーザを認証するための認証キーとして利用することも可能である。

【０００５】例えば、コンサートの開催主が、コンサート会場に入場しようとするユーザに対して、認証キーとなる２次元コードを配布するなどの利用方法が考えられる。この場合、コンサートの開催主は、コンサートの入場チケットを購入したユーザに対して、固有のコード番号を割り当てる。そして、開催主は、２次元コードを生成するためのプログラムを実行し、コード番号を入力することによって、所定の２次元コードを生成し、認証キーとしてユーザに配布する。２次元コードが配布されたユーザは、コンサート会場にて、そのコードを提示して、所定の認識端末にて認証されると、入場が許可される。

【０００６】

【発明が解決しようとする課題】しかしながら、上述したプログラムは、入力されたコード番号を意味する２次元コードを生成するものであるため、コード番号さえわかれば、第３者によって、不正に同一の２次元コードが生成され、利用されてしまう恐れがあった。

【０００７】また、２次元コードが印刷された媒体もしくは２次元コードの画像データが第３者の手に渡ってしまうと、いわゆる「なりすまし」が可能になってしまう課題があった。

【０００８】本発明はこのような状況に鑑みてなされたものであり、２次元コードを生成するためのプログラム自体をユーザ毎に変化させて、それを認証キーとして機能させ、そのプログラムを所有するユーザのみが所定の２次元コードを作成することにより、高精度にユーザ認証することができるようにするものである。

【０００９】

【課題を解決するための手段】本発明の情報提供装置は、情報処理装置から送信されてくるプログラムの発行要求を受けて、情報処理装置に対して、ユーザIDを発行する発行手段と、発行手段により発行されたユーザID、および発行要求の受信時刻を基に、乱数を発生する乱数発生手段と、乱数発生手段により発生された乱数、ユーザID、および受信時刻を基に、所定画像を生成するためのプログラムを作成する作成手段と、作成手段により作成されたプログラムを情報処理装置に提供する提供手段とを備えることを特徴とする。

【００１０】ユーザIDに対応付けて、乱数および受信時刻を記録する記録手段をさらに設けるようにすることができる。

【００１１】所定画像は、２次元コードであるものとすることができる。

【００１２】本発明の情報提供方法は、情報処理装置から送信されてくるプログラムの発行要求を受けて、情報処理装置に対して、ユーザIDを発行する発行処理ステップと、発行処理ステップの処理により発行されたユーザID、および発行要求の受信時刻を基に、乱数を発生する乱数発生処理ステップと、乱数発生処理ステップの処理により発生された乱数、ユーザID、および受信時刻を基に、所定画像を生成するためのプログラムを作成する作成処理ステップと、作成処理ステップの処理により作成されたプログラムを情報処理装置に提供する提供処理ステップとを含むことを特徴とする。

【００１３】本発明の第１の記録媒体に記録されているプログラムは、情報処理装置から送信されてくるプログラムの発行要求を受けて、情報処理装置に対して、ユーザIDを発行する発行処理ステップと、発行処理ステップの処理により発行されたユーザID、および発行要求の受信時刻を基に、乱数を発生する乱数発生処理ステップと、乱数発生処理ステップの処理により発生された乱数、ユーザID、および受信時刻を基に、所定画像を生成するためのプログラムを作成する作成処理ステップと、作成処理ステップの処理により作成されたプログラムを情報処理装置に提供する提供処理ステップとを含むことを特徴とする。

【００１４】本発明の第１のプログラムは、情報処理装置から送信されてくるプログラムの発行要求を受けて、情報処理装置に対して、ユーザIDを発行する発行処理ステップと、発行処理ステップの処理により発行されたユーザID、および発行要求の受信時刻を基に、乱数を発生する乱数発生処理ステップと、乱数発生処理ステップの処理により発生された乱数、ユーザID、および受信時刻を基に、所定画像を生成するためのプログラムを作成する作成処理ステップと、作成処理ステップの処理により作成されたプログラムを情報処理装置に提供する提供処理ステップとをコンピュータに実行させることを特徴とする。

【００１５】本発明の情報提供装置および方法、並びに第１のプログラムにおいては、情報処理装置から送信されてくるプログラムの発行要求を受けて、情報処理装置に対して、ユーザIDが発行され、発行されたユーザID、および発行要求の受信時刻を基に、乱数が発生され、発生された乱数、ユーザID、および受信時刻を基に、所定画像を生成するためのプログラムが作成され、作成されたプログラムが情報処理装置に提供される。

【００１６】本発明の情報処理装置は、情報提供装置に対してプログラムの送信を要求する要求手段と、要求手段に基づいて情報提供装置から提供されるプログラムを受信する受信手段と、受信手段により受信されたプログラムを実行し、所定画像を生成する生成手段と、生成手段により生成された所定画像を表示する表示手段とを備えることを特徴とする。

【００１７】生成手段には、プログラムの実行時刻を基に、所定画像を生成させることができる。

【００１８】生成手段には、所定時間毎に所定画像を生

成させるようにし、表示手段には、生成手段により所定時間毎に生成される所定画像を表示させることができる。

【００１９】所定画像は、２次元コードであるものとすることができ、２次元コードには、ユーザIDを示すコード情報が含まれているものとすることができる。

【００２０】本発明の情報処理方法は、情報提供装置に対してプログラムの送信を要求する要求処理ステップと、要求処理ステップの処理に基づいて情報提供装置から提供されるプログラムを受信する受信処理ステップと、受信処理ステップの処理により受信されたプログラムを実行し、所定画像を生成する生成処理ステップと、生成処理ステップの処理により生成された所定画像を表示する表示処理ステップとを含むことを特徴とする。

【００２１】本発明の第２の記録媒体に記録されいているプログラムは、情報提供装置に対してプログラムの送信を要求する要求処理ステップと、要求処理ステップの処理に基づいて情報提供装置から提供されるプログラムを受信する受信処理ステップと、受信処理ステップの処理により受信されたプログラムを実行し、所定画像を生成する生成処理ステップと、生成処理ステップの処理により生成された所定画像を表示する表示処理ステップとを含むことを特徴とする。

【００２２】本発明の第２のプログラムは、情報提供装置に対してプログラムの送信を要求する要求処理ステップと、要求処理ステップの処理に基づいて情報提供装置から提供されるプログラムを受信する受信処理ステップと、受信処理ステップの処理により受信されたプログラムを実行し、所定画像を生成する生成処理ステップと、生成処理ステップの処理により生成された所定画像を表示する表示処理ステップとをコンピュータに実行させることを特徴とする。

【００２３】本発明の情報処理装置および方法、並びに第２のプログラムにおいては、情報提供装置に対してプログラムの送信が要求され、情報提供装置から提供されるプログラムが受信され、受信されたプログラムが実行されて所定画像が生成され、生成された所定画像が表示される。

【００２４】本発明の情報認証装置は、第１の画像を撮像する撮像手段と、撮像手段により撮像された第１の画像に対応する第１の情報を認識する認識手段と、認識手段により認識された第１の情報に含まれるユーザIDを基に、他の装置に記録されているユーザ情報を検索する検索手段と、検索手段により検索されたユーザ情報を基に、第２の画像を生成するためのプログラムを作成する作成手段と、作成手段により作成されたプログラムを実行し、第２の画像を生成する生成手段と、生成手段により生成された第２の画像に対応する第２の情報と、認識手段により認識された第１の情報を認証する認証手段とを備えることを特徴とする。

【００２５】撮像手段には、情報処理装置の表示部に表示されている第１の画像を撮像させることができる。

【００２６】ユーザ情報は、少なくとも乱数および時刻情報を含むようにすることができ、検索手段には、ユーザIDを基に、乱数および時刻情報を検索させ、作成手段には、検索手段により検索された乱数および時刻情報、並びにユーザIDを基に、第２の画像を生成するためのプログラムを作成させることができる。

【００２７】生成手段には、プログラムの実行時刻を基に、第２の画像を生成させることができる。

【００２８】第１の画像および第２の画像は、２次元コードであるものとすることができ、第１の情報および第２の情報は、コード番号を示す情報であるものとすることができる。

【００２９】本発明の情報認証方法は、第１の画像を撮像する撮像処理ステップと、撮像処理ステップの処理により撮像された第１の画像に対応する第１の情報を認識する認識処理ステップと、認識処理ステップの処理により認識された第１の情報に含まれるユーザIDを基に、他の装置に記録されているユーザ情報を検索する検索処理ステップと、検索処理ステップの処理により検索されたユーザ情報を基に、第２の画像を生成するためのプログラムを作成する作成処理ステップと、作成処理ステップの処理により作成されたプログラムを実行し、第２の画像を生成する生成処理ステップと、生成処理ステップの処理により生成された第２の画像に対応する第２の情報と、認識処理ステップの処理により認識された第１の情報を認証する認証処理ステップとを含むことを特徴とする。

【００３０】本発明の第３の記録媒体に記録されているプログラムは、第１の画像を撮像する撮像処理ステップと、撮像処理ステップの処理により撮像された第１の画像に対応する第１の情報を認識する認識処理ステップと、認識処理ステップの処理により認識された第１の情報に含まれるユーザIDを基に、他の装置に記録されているユーザ情報を検索する検索処理ステップと、検索処理ステップの処理により検索されたユーザ情報を基に、第２の画像を生成するためのプログラムを作成する作成処理ステップと、作成処理ステップの処理により作成されたプログラムを実行し、第２の画像を生成する生成処理ステップと、生成処理ステップの処理により生成された第２の画像に対応する第２の情報と、認識処理ステップの処理により認識された第１の情報を認証する認証処理ステップとを含むことを特徴とする。

【００３１】本発明の第３のプログラムは、第１の画像を撮像する撮像処理ステップと、撮像処理ステップの処理により撮像された第１の画像に対応する第１の情報を認識する認識処理ステップと、認識処理ステップの処理により認識された第１の情報に含まれるユーザIDを基に、他の装置に記録されているユーザ情報を検索する検

索処理ステップと、検索処理ステップの処理により検索されたユーザ情報を基に、第２の画像を生成するためのプログラムを作成する作成処理ステップと、作成処理ステップの処理により作成されたプログラムを実行し、第２の画像を生成する生成処理ステップと、生成処理ステップの処理により生成された第２の画像に対応する第２の情報と、認識処理ステップの処理により認識された第１の情報を認証する認証処理ステップとをコンピュータに実行させることを特徴とする。

【００３２】本発明の情報認証装置および方法、並びに第３のプログラムにおいては、第１の画像が撮像され、撮像された第１の画像に対応する第１の情報が認識され、認識された第１の情報に含まれるユーザIDを基に、他の装置に記録されているユーザ情報が検索され、検索されたユーザ情報を基に、第２の画像を生成するためのプログラムが作成され、作成されたプログラムが実行されて第２の画像が生成され、生成された第２の画像に対応する第２の情報と、認識された第１の情報が認証される。

【００３３】本発明の認証システムは、情報提供装置が、情報処理装置から送信されてくるプログラムの発行要求を受けて、情報処理装置に対して、ユーザIDを発行する発行手段と、発行手段により発行されたユーザID、および発行要求の受信時刻を基に、乱数を発生する乱数発生手段と、乱数発生手段により発生された乱数、ユーザID、および受信時刻を基に、第１の画像を生成するための第１のプログラムを作成する第１の作成手段と、第１の作成手段により作成された第１のプログラムを情報処理装置に提供する提供手段と、ユーザIDに対応付けて、乱数および受信時刻を記録する記録手段とを備え、情報処理装置が、情報提供装置に対して第１のプログラムの送信を要求する要求手段と、情報提供装置から提供される第１のプログラムを受信する受信手段と、受信手段により受信された第１のプログラムを実行し、第１の画像を生成する第１の生成手段と、第１の生成手段により生成された第１の画像を表示する表示手段とを備え、情報認証装置が、情報処理装置の表示手段に表示されている第１の画像を撮像する撮像手段と、撮像手段により撮像された第１の画像に対応する第１の情報を認識する認識手段と、認識手段により認識された第１の情報に含まれるユーザIDを基に、情報提供装置の記録手段に記録されている乱数および受信時刻を検索する検索手段と、検索手段により検索された乱数および受信時刻を基に、第２の画像を生成するための第２のプログラムを作成する第２の作成手段と、第２の作成手段により作成された第２のプログラムを実行し、第２の画像を生成する第２の生成手段と、第２の生成手段により生成された第２の画像に対応する第２の情報と、認識手段により認識された第１の情報を認証する認証手段とを備えることを特徴とする。

【００３４】第１の生成手段には、第１のプログラムの実行時刻を基に、第１の画像を生成させ、第２の生成手段には、第２のプログラムの実行時刻を基に、第２の画像を生成させることができる。

【００３５】第１の画像および第２の画像は、２次元コードであるものとすることができる。

【００３６】本発明の認証システムにおいては、情報提供装置で、情報処理装置から送信されてくるプログラムの発行要求を受けて、情報処理装置に対して、ユーザIDが発行され、発行されたユーザID、および発行要求の受信時刻を基に、乱数が発生され、発生された乱数、ユーザID、および受信時刻を基に、第１の画像を生成するための第１のプログラムが作成され、作成された第１のプログラムが情報処理装置に提供され、ユーザIDに対応付けて、乱数および受信時刻が記録され、情報処理装置で、情報提供装置に対して第１のプログラムの送信が要求され、情報提供装置から提供される第１のプログラムが受信され、受信された第１のプログラムが実行されて第１の画像が生成され、生成された第１の画像が表示され、情報認証装置で、情報処理装置に表示されている第１の画像が撮像され、撮像された第１の画像に対応する第１の情報が認識され、認識された第１の情報に含まれるユーザIDを基に、情報提供装置に記録されている乱数および受信時刻が検索され、検索された乱数および受信時刻を基に、第２の画像を生成するための第２のプログラムが作成され、作成された第２のプログラムが実行されて第２の画像が生成され、生成された第２の画像に対応する第２の情報と、認識された第１の情報が認証される。

【００３７】

【発明の実施の形態】以下、図を参照して、本発明の実施の形態について説明する。

【００３８】図１は、本発明を適用したチケットレスシステムの一実施の形態の構成例を示す図である。

【００３９】カメラ付デジタル携帯電話機１（以下、単に携帯電話機１と称する）は、通信サービスの提供エリアを所望の広さに分割したセルにそれぞれ配置されている、固定無線端末である基地局２を介して、公衆回線網５に接続されている。

【００４０】基地局２は、移動無線端末である携帯電話機１を、例えば、W-CDMA（Wideband-Code Division Multiple Access）と呼ばれる符号分割多元接続により無線接続し、携帯電話機１と、2GHzの周波数帯域を利用して最大2Mbpsのデータ転送速度で大容量データを高速にデータ通信できる。

【００４１】また、基地局２は、有線回線を介して、公衆回線網５に接続されている。公衆回線網５は、インターネットサービスプロバイダ６を介してインターネット７に接続されているほか、図示せぬ加入者有線端末装置、コンピュータネットワーク、および企業内ネットワ

ーク等に接続されている。

【００４２】携帯電話機１は、基地局２とW-CDMA方式により大容量データを高速にデータ通信できるので、電子メールの送受信、簡易ホームページの閲覧、画像の送受信等の多種に及ぶデータ通信を実行することができる。

【００４３】携帯電話機１はまた、ｉ－アプリ（登録商標）機能を有しており、サイバーコード認証サイト８から提供される様々な、Java（登録商標）言語で記述されたプログラム（いわゆるJava（登録商標）アプレット）をダウンロードすることができる。

【００４４】例えば、携帯電話機１は、公衆回線網５、インターネットサービスプロバイダ６、およびインターネット７を介して、サイバーコード認証サイト８に接続し、所定の２次元コードを生成するためのプログラム（Java（登録商標）アプレット）をダウンロードすることができる。携帯電話機１は、ダウンロードされたプログラムを実行して２次元コードを生成し、生成された２次元コードを液晶ディスプレイ３５（図３）に表示させる。液晶ディスプレイ３５に表示された２次元コードは、後述するように、コンサート会場４に入場するための入場チケットの代替（認証キー）として利用される。

【００４５】本発明では、この２次元コードの一種として、本出願人によって開発されたサイバーコード（CyberCode）（登録商標）を例に挙げて説明する。

【００４６】チケットレス端末３は、CCD（Charge Coupled Device）カメラ１０７（図７）を有するパーソナルコンピュータなどで構成され、コンサート会場４の入口付近に設けられる。チケットレス端末３は、携帯電話機１の液晶ディスプレイ３５に表示されたサイバーコードをCCDカメラ１０７で撮像し、その結果得られるサイバーコードの画像データから、サイバーコードのコードパターンを認識し、そのコードパターンに対応した所定の処理を実行するようになされている。

【００４７】例えば、チケットレス端末３は、コードパターンから得られるコード番号を、公衆回線網５乃至インターネット７を介してサイバーコード認証サイト８に送信し、ユーザ認証を行うように要求する。チケットレス端末３は、サイバーコード認証サイト８から供給される認証結果を受信し、液晶ディスプレイ１０９（図７）に表示させることができる。

【００４８】インターネット７には、インターネットサービスプロバイダ６、サイバコード認証サイト８、WWW（World Wide Web）サーバ９－１，９－２（以下、これらのWWWサーバ９－１，９－２を個々に区別する必要がない場合、単にWWWサーバ９と称する）、および、企業１０が接続されている。

【００４９】サイバーコード認証サイト８は、サイバーコード生成プログラム発行／認証サーバ１１および登録ユーザ情報データベース（DB）１２などで構成される。サイバーコード生成プログラム発行／認証サーバ１１は、携帯電話機１のユーザから、予め、住所、氏名、および電話番号などのユーザ情報の登録を受け付けておき、それらの情報を、登録ユーザ情報データベース１２に記録するようになされている。

【００５０】図２は、登録ユーザ情報データベース１２に記録されているユーザ情報の記録例を示す図である。同図においては、サイバーコード生成プログラムの発行要求があったユーザに割り当てられるユーザIDがユーザ情報と関連付けられて記録されるとともに、ユーザIDに対応付けてサイバーコード生成プログラムの発行開始時刻TID、および乱数発生用SeedIDが記録される。

【００５１】ユーザ情報は、主に、発行されたサイバーコードを生成するためのプログラム（認証用サイバーチケット）の決済を行うときなどに利用され、ユーザ情報を基に、所定のクレジット会社や銀行などに照会され、決済が実行される。

【００５２】サイバーコード生成プログラム発行／認証サーバ１１は、サイバーコード生成プログラムの発行を希望するユーザからユーザIDの登録を受け付けると、ユーザ毎に固有の識別子であるユーザID（UID）を発行し、ユーザ情報に対応付けて、発行されたユーザIDを登録ユーザ情報データベース１２に記録させるとともに、ユーザIDを、インターネット７を介して携帯電話機１に通知（送信）するようになされている。

【００５３】サイバーコード生成プログラム発行／認証サーバ１１は、携帯電話機１からユーザIDを含むサイバーコード生成プログラムの送信（発行）要求を受けて、シード（Seed）作成プログラムを起動し、受信したユーザID、および現在時刻TIDから乱数発生用SeedIDを作成するようになされている。

【００５４】サイバーコード生成プログラム発行／認証サーバ１１は、作成された乱数発生用SeedID、ユーザID、および現在時刻TIDからサイバーコード生成プログラムを作成し、インターネット７を介して、携帯電話機１に送信した後、ユーザIDに対応付けて、サイバーコード発行開始時刻TIDおよび作成された乱数発生用SeedIDを、登録ユーザ情報データベース１２に登録（記録）するようになされている。

【００５５】なお、乱数発生用SeedIDは、サイバーコード（すなわちコード番号）をランダムに生成することができるように、サイバーコード生成プログラム毎に固有の値とされ、登録ユーザ情報データベース１２で管理される。しかしながら、乱数発生用SeedIDが漏洩されると、セキュリティ上好ましくない場合があるため、乱数発生用SeedIDを作成するときに用いられるデータ（ユーザIDおよびサイバーコード発行開始時刻TID）のみを登録ユーザ情報データベース１２で管理させるようにして、乱数発生用SeedIDの漏洩を防止するようにしてもよい。

【００５６】サイバーコード生成プログラム発行／認証

サーバ１１は、チケットレス端末３から送信されてくるコード番号（すなわち、携帯電話機１の液晶ディスプレイ３５に表示されたサイバーコードがCCDカメラ１０７で認識され、認識されたコードパターンに対応するコード番号）を受けて、認証用キー分離プログラムを起動し、コード番号に含まれるユーザIDを分離するようになされている。

【００５７】サイバーコード生成プログラム発行／認証サーバ１１は、分離されたユーザIDを基に、登録ユーザ情報データベース１２から、対応するユーザIDの発行開始時刻TIDおよび乱数発生用SeedIDを検索し、再度、サイバーコード生成プログラムを作成するようになされている。サイバーコード生成プログラム発行／認証サーバ１１は、作成されたサイバーコード生成プログラムを実行することにより生成されるサイバーコードを基に、ユーザ認証処理を実行するようになされている。

【００５８】サイバーコード生成プログラム発行／認証サーバ１１は、インターネット７を介して企業１０が有するパーソナルコンピュータ１３と接続され、パーソナルコンピュータ１３から認証用サイバーチケット発行の依頼を受けて、上述したようにして、特定のユーザに対してサイバーコード生成プログラムを発行したり、企業１０に対して、課金処理を実行するようになされている。

【００５９】WWWサーバ９は、TCP/IP（Transmission Control Protocol/Internet Protocol）のプロトコルに従って、携帯電話機１、もしくは企業１０が有するパーソナルコンピュータ１３からアクセスされ、インターネット７を介して、各種のホームページに代表される情報を提供する。提供される情報は、例えば、HTML（HyperText Markup Language）、XML（eXtensible Markup Language）、あるいは、コンパクトHTMLなどのページ記述言語で記述されている。ここでは、WWWサーバ９－１，９－２しか図示していないが、複数のWWWサーバ９が接続されることは言うまでもない。

【００６０】企業１０は、例えば、コンサート会場４で開催されるコンサートの開催主である。企業１０は、パーソナルコンピュータ１３を用いて、インターネット７を介して、サイバーコード認証サイト８に認証用サイバーチケットの発行およびユーザ認証を依頼したり、チケット発行の費用の請求を受ける。企業１０はまた、ネットワークを介さずに、その他の方法を用いて（すなわち、オフラインで）、サイバーコード認証サイト８に認証用サイバーチケットの発行およびユーザ認証を依頼したり、チケット発行の費用の請求を受けるようにしてもよい。

【００６１】図３は、携帯電話機１の外観の構成例を示す図である。同図に示されるように、携帯電話機１は、表示部２２および本体２３で構成され、中央のヒンジ部２１により折り畳み可能に形成されている。

【００６２】表示部２２は、上端左部に引出しまたは収納可能な送受信用のアンテナ３１を有する。携帯電話機１は、アンテナ３１を介して、固定無線局である基地局２との間で電波を送受信する。

【００６３】また、表示部２２は、上端中央部にほぼ１８０度の角度範囲で回動自在なカメラ部３２を有する。携帯電話機１は、カメラ部３２のCCDカメラ３３によって所望の撮像対象を撮像する。

【００６４】カメラ部３２が使用者によってほぼ１８０度回動されて位置決めされた場合、図４に示すように、表示部２２は、カメラ部３２の背面側中央に設けられたスピーカ３４が正面側に位置する状態となる。これにより、携帯電話機１は、通常の音声通話状態に切り換わる。

【００６５】さらに、表示部２２の正面に液晶ディスプレイ３５が設けられている。液晶ディスプレイ３５は、電波の受信状態、電池残量、電話帳として登録されている相手先名や電話番号および発信履歴等の他、電子メールの内容、簡易ホームページ、カメラ部３２のCCDカメラ３３で撮像した画像などを表示する。

【００６６】一方、本体２３には、その表面に「０」乃至「９」の数字キー、発呼キー、リダイヤルキー、終話及び電源キー、クリアキー及び電子メールキー等の操作キー４１が設けられている。操作キー４１の操作に対応した各種指示が、携帯電話機１に入力される。

【００６７】また、本体２３の操作キー４１の下部にメモボタン４２およびマイクロフォン４３が設けられている。携帯電話機１は、メモボタン４２が操作されたとき、通話中の相手の音声を録音する。携帯電話機１は、マイクロフォン４３によって通話時の使用者の音声を集音する。

【００６８】さらに、本体２３の操作キー４１の上部に回動自在なジョグダイヤル４４が、本体２３の表面から僅かに突出した状態で設けられている。携帯電話機１は、ジョグダイヤル４４に対する回動操作に応じて、液晶ディスプレイ３５に表示されている電話帳リストもしくは電子メールのスクロール動作、簡易ホームページのページ捲り動作、または画像の送り動作等の種々の動作を実行する。

【００６９】例えば、本体２３は、使用者によるジョグダイヤル４４の回動操作に応じて液晶ディスプレイ３５に表示された電話帳リストの複数の電話番号の中から所望の電話番号を選択し、ジョグダイヤル４４が本体２３の内部方向に押圧されたとき、選択されている電話番号を確定して、確定した電話番号に対して自動的に発呼処理を行う。

【００７０】なお、本体２３は、背面側に図示せぬバッテリパックが装着されており、終話／電源キーがオン状態になると、バッテリパックから各回路部に対して電力が供給されて動作可能な状態に起動する。

【００７１】ところで、本体２３の左側面上部に抜差自在なメモリカード５１を装着するためのメモリカードスロット４５が設けられている。携帯電話機１は、メモボタン４２が押下されると、通話中の相手の音声を装着されているメモリカード５１に記録する。携帯電話機１は、使用者の操作に応じて、電子メール、簡易ホームページ、CCDカメラ３３で撮像した画像を、装着されているメモリカード５１に記録する。

【００７２】同図に示されるメモリカード５１は、例えば、メモリースティック（商標）と呼ばれる本出願人によって開発されたフラッシュメモリカードの一種である。このメモリカード５１は、縦21.5×横50×厚さ2.8[mm]の小型薄型形状のプラスチックケース内に電気的に書換えや消去が可能な不揮発性メモリであるEEPROM（Electrically Erasable and Programmable Read Only Memory）の一種であるフラッシュメモリ素子を格納したものであり、１０ピン端子を介して画像や音声、音楽等の各種データの書き込みおよび読み出しが可能となっている。

【００７３】またメモリカード５１は、大容量化等による内蔵フラッシュメモリの仕様変更に対しても、使用する機器で互換性を確保することができる独自のシリアルプロトコルを採用し、最大書込速度1.5[MB/S]、最大読出速度2.45[MB/S]の高速性能を実現しているとともに、誤消去防止スイッチを設けて高い信頼性を確保している。

【００７４】従って、携帯電話機１は、このようなメモリカード５１を装着可能に構成されているために、メモリカード５１を介して、他の電子機器との間でデータの共有化を図ることができる。

【００７５】図５に示すように、携帯電話機１は、表示部２２および本体２３の各部を統括的に制御する主制御部６１に対して、電源回路部６５、操作入力制御部６２、画像エンコーダ６３、カメラインターフェース（I/F）部６４、LCD（Liquid Crystal Display）制御部６６、画像デコーダ６７、多重分離部６８、記憶再生部７３、変復調回路部６９、および音声コーデック７０がメインバス７１を介して互いに接続されるとともに、画像エンコーダ６３、画像デコーダ６７、多重分離部６８、変復調回路部６９、および音声コーデック７０が同期バス７２を介して互いに接続されて構成されている。

【００７６】電源回路部６５は、使用者の操作により終話／電源キーがオン状態にされると、バッテリパックから各部に対して電力を供給することにより、携帯電話機１を動作可能な状態に起動する。

【００７７】携帯電話機１は、CPU（Central Processing Unit），ROM（Read Only Memory）およびRAM（Random Access Memory）等でなる主制御部６１の制御に基づいて、音声通話モードにおいて、マイクロフォン４３で集音した音声信号を音声コーデック７０によってデジタル音声データに変換する。携帯電話機１は、デジタル音声データを変復調回路部６９でスペクトラム拡散処理し、送受信回路部７４でデジタルアナログ変換処理および周波数変換処理を施した後にアンテナ３１を介して送信する。

【００７８】また、携帯電話機１は、音声通話モードにおいて、アンテナ３１で受信した受信信号を増幅して周波数変換処理およびアナログデジタル変換処理を施し、変復調回路部６９でスペクトラム逆拡散処理し、音声コーデック７０によってアナログ音声信号に変換する。携帯電話機１は、アナログ音声信号に対応する音声をスピーカ３４に出力させる。

【００７９】さらに、携帯電話機１は、データ通信モードにおいて、電子メールを送信する場合、操作キー４１およびジョグダイヤル４４の操作によって入力された電子メールのテキストデータを操作入力制御部６２を介して主制御部６１に送出する。

【００８０】主制御部６１は、テキストデータを変復調回路部６９でスペクトラム拡散処理し、送受信回路部７４でデジタルアナログ変換処理および周波数変換処理を施した後にアンテナ３１を介して基地局２へ送信する。

【００８１】これに対して携帯電話機１は、データ通信モードにおいて、電子メールを受信する場合、アンテナ３１を介して基地局２から受信した受信信号を変復調回路部６９でスペクトラム逆拡散処理して、元のテキストデータを復元した後、LCD制御部６６を介して液晶ディスプレイ３５に電子メールとして表示する。

【００８２】この後、携帯電話機１は、使用者の操作に応じて受信した電子メールを、記憶再生部７３を介してメモリカード５１に記録することも可能である。

【００８３】携帯電話機１は、データ通信モードにおいて画像データを送信する場合、CCDカメラ３３で撮像された画像データを、カメラインターフェース部６４を介して画像エンコーダ６３に供給する。

【００８４】因みに携帯電話機１は、画像データを送信しない場合には、CCDカメラ３３で撮像した画像データを、カメラインターフェース部６４およびLCD制御部６６を介して液晶ディスプレイ３５に直接表示することも可能である。

【００８５】画像エンコーダ６３は、CCDカメラ３３から供給された画像データを、例えば、MPEG（Moving Picture Experts Group）２またはMPEG4等の所定の符号化方式によって圧縮符号化することにより符号化画像データに変換し、これを多重分離部６８に送出する。

【００８６】このとき同時に携帯電話機１は、CCDカメラ３３で撮像中にマイクロフォン４３で集音した音声を、音声コーデック７０を介してデジタルの音声データとして多重分離部６８に送出する。

【００８７】多重分離部６８は、画像エンコーダ６３から供給された符号化画像データと音声コーデック７０か

ら供給された音声データとを所定の方式で多重化し、その結果得られる多重化データを変復調回路部６９でスペクトラム拡散処理し、送受信回路部７４でデジタルアナログ変換処理および周波数変換処理を施した後にアンテナ３１を介して送信する。

【００８８】これに対して携帯電話機１は、データ通信モードにおいて、例えば、簡易ホームページ等にリンクされた動画像ファイルのデータを受信する場合、アンテナ３１を介して基地局２から受信した受信信号を変復調回路部６９でスペクトラム逆拡散処理し、その結果得られる多重化データを多重分離部６８に送出する。

【００８９】多重分離部６８は、多重化データを符号化画像データと音声データとに分離し、同期バス７２を介して、符号化画像データを画像デコーダ６７に供給するとともに、音声データを音声コーデック７０に供給する。

【００９０】画像デコーダ６７は、符号化画像データをMPEG2またはMPEG4等の所定の符号化方式に対応した復号方式でデコードすることにより再生動画像データを生成し、これをLCD制御部６６を介して液晶ディスプレイ３５に供給する。これにより、携帯電話機１は、例えば、簡易ホームページにリンクされた動画像ファイルに含まれる動画データを表示する。

【００９１】このとき同時に音声コーデック７０は、音声データをアナログ音声信号に変換した後、これをスピーカ３４に供給する。これにより、携帯電話機１は、例えば、簡易ホームページにリンクされた動画像ファイルに含まる音声データを再生する。

【００９２】この場合も電子メールの場合と同様に、携帯電話機１は、受信した簡易ホームページ等にリンクされたデータを使用者の操作により記憶再生部７３を介してメモリカード５１に記録することが可能である。

【００９３】図６は、携帯電話機１の機能を説明するブロック図である。

【００９４】入出力制御プログラム８１は、操作キー４１もしくはジョグダイヤル４４を用いて、ユーザが入力した操作または命令を示す信号を、対応するアプリケーションに供給したり、各種アプリケーションの処理に基づいて、マイクロフォン４３から入力されたユーザの音声データなどをスピーカ３４に出力して音声を再生させたり、CCDカメラ３３で撮像された画像データなどを液晶ディスプレイ３５に出力して画像を表示させたり、所定のデータをメモリカード５１に供給してそこに記録させたり、所定のデータを、データ通信プログラム８７を介してアンテナ３１に出力して対応する電波を出力させる処理を制御するプログラムである。

【００９５】ウェブブラウザ８２は、WWWサーバ９の情報をクライアント側でブラウズするためのソフトウェアプログラムである。WWWサーバ９とWWWクライアント間で、所定の通信プロトコルに基づいて通信を実行し、さらにセキュリティ機能や音声／動画などのマルチメディアデータの再生、WWWサーバ９とWWWクライアントとの間でプログラム転送を可能にする拡張言語（例えば、Java（登録商標））などをサポートするものである。

【００９６】表示プログラム８３は、メモリカード５１に記録されている画像データもしくはCCDカメラ３３で撮像された画像データを、入出力制御プログラム８１の処理により液晶ディスプレイ３５に表示させるために、データを変換したり、画像処理を実行するためのプログラムである。

【００９７】電子メールプログラム８４は、インターネットサービスプロバイダ６に対し、自分宛の電子メールを送信するように要求し、自分宛の電子メールをダウンロード（受信）するプログラムである。電子メールプログラム８４はまた、インターネットサービスプロバイダ６に対し、所定の宛先に電子メールを送信するように要求するプログラムである。

【００９８】Java（登録商標）アプレット実行プログラム８５は、サイバーコード認証サイト８にアクセスし、所定のJava（登録商標）アプレットをダウンロードする際に必要となるユーザIDを登録したり、所定のJava（登録商標）アプレットをダウンロードする処理を実行するプログラムである。

【００９９】Java（登録商標）アプレット実行プログラム８５はまた、サイバーコード認証サイト８からダウンロードされ、メモリ８６に記憶されているJava（登録商標）アプレット９１－１および９１－２の中から、ユーザの操作によっていずれかが選択されると、選択されたJava（登録商標）アプレットを実行する。例えば、後述するように、Java（登録商標）アプレット（サイバーコード生成プログラム）の実行によって、認証用のサイバーコード（認証用サイバーチケット）が生成され、生成されたサイバーコードが液晶ディスプレイ３５に表示される。

【０１００】データ通信プログラム８７は、主制御部６１が実行しているアプリケーション（例えば、ウェブブラウザ８２）において、アンテナ３１を介して、他の装置と情報の通信を行う場合、その通信を制御するプログラムである。

【０１０１】図７乃至図９は、図１のチケットレス端末３の構成例を示す図である。このチケットレス端末装置３は、基本的に、本体１０１と本体１０１に対して開閉自在に取り付けられた表示部１０２により構成されている。

【０１０２】本体１０１は、その上面に各種文字や記号および数字などを入力するとき操作される操作キー１０３、マウスカーソルの移動に用いられるスティック式ポインティングディバイス（以下、適宜、スティックと称する）１０４、通常のマウスにおける左ボタンおよび右ボタンに相当する左クリックボタン１０４Ａおよび１０

４Ｂ、マウスカーソルをスクロールボタンに合わせることなくスクロールバーを操作するためのセンタボタン１０４Ｃ、内蔵スピーカ１０５Ａおよび１０５Ｂ、押圧式の電源スイッチ１０６、表示部１０２に設けられたCCDカメラ１０７用のシャッタボタン１０８、LED（Light Emitting Diode）で構成された電源ランプPL、電池ランプBLおよびメッセージランプMLなどが設けられている。

【０１０３】表示部１０２の正面には、例えば、TFT（Thin Film Transistor）カラー液晶でなる液晶ディスプレイ１０９が設けられており、その中央上端部にはCCDカメラ１０７を備えた撮像部１１１が表示部１０２に対して回動自在に設けられている。すなわち、この撮像部１１１は、表示部１０２と同一の方向と、その逆の方向（背面の方向）との間の１８０度の範囲の任意の位置に回動することができるようになされている。撮像部１１１には、調整リング１１２によりフォーカスの調整が可能なようになされている。

【０１０４】また表示部１０２は、撮像部１１１の左端近傍における正面側および背面側にマイクロフォン１１３が設けられており、マイクロフォン１１３を介して表示部１０２の正面側から背面側までの広範囲に渡って集音するようになされている。

【０１０５】さらに表示部１０２は、液晶ディスプレイ１０９の左端近傍および右端近傍にそれぞれツメ１１４および１１５が設けられ、ツメ１１４および１１５と対応する本体１０１の所定位置には、孔部１１６および１１７がそれぞれ設けられており、表示部１０２を本体１０１に閉塞した状態でツメ１１４および１１５がそれぞれ対応する孔部１１６および１１７に嵌合される。

【０１０６】これに対して表示部１０２は、本体１０１に閉塞された表示部１０２の前側が持ち上げられたときに、孔部１１６および１１７とツメ１１４および１１５の嵌合状態が解除され、表示部１０２が本体１０１から展開される。

【０１０７】また本体１０１は、その右側面にIrDA（Infrared Data Association）準拠の赤外線ポート１１８、ヘッドフォン端子１１９、マイクロフォン用入力端子１２０、USB（Universal Serial Bus）端子１２１、外部電源コネクタ１２２、外部ディスプレイ出力用コネクタ１２３、回転操作子の回転操作および押圧操作によって所定の処理を実行するための命令を入力するジョグダイヤル１２４およびモジュラジャック用のモデム端子１２５が設けられている。

【０１０８】また本体１０１は、その左側面に排気孔１２６、PCMCIA（Personal ComputerMemory Card International Association）規格のPC（Personal Computer）カードに対応したPCカードスロット１２７および４ピン対応のIEEE（Institute of Electrical and Electronics Engineers）1394端子１２８が設けられている。

【０１０９】さらに本体１０１は、その後側面にバッテリコネクタ１２９が設けられており、底面にはバッテリパック１３０を取り外すためのスライド式取り外しレバー１３１、およびスライド式取り外しレバー１３１のスライド操作をロックするロックレバー１３２が設けられるとともに、本体１０１の動作を中断して電源投入時の環境を再構築するためのリセットスイッチ１３３が設けられている。なお、バッテリパック１３０は、バッテリコネクタ１２９に対して着脱自在に接続される。

【０１１０】図１０は、チケットレス端末３の内部の構成例を示す図である。

【０１１１】本体１０１の各種機能を統括的に制御するCPU１５０がホストバス１５２に接続されており、CPU１５０によってRAM１５３にロードされた各種プログラムやアプリケーションソフトウェアに応じた処理を、クロックジェネレータ１６０から与えられるシステムクロックに基づいて、所定の動作速度で実行することにより各種機能を実現するようになされている。またホストバス１５２には、キャッシュメモリ１５１が接続されており、CPU１５０が使用するデータをキャッシュし、高速アクセスを実現するようになされている。

【０１１２】このホストバス１５２は、PCI（Peripheral Component Interconnect）バス１５５とホストーPCIブリッジ１５４を介して接続されており、PCIバス１５５にはビデオコントローラ１５６、IEEE1394インターフェース１５７、ビデオキャプチャ処理チップ１８３およびPCカードインターフェース１５８が接続されている。

【０１１３】ここでホストーPCIブリッジ１５４は、CPU１５０と、ビデオコントローラ１５６、ビデオキャプチャ処理チップ１８３、IEEE1394インターフェース１５７およびPCカードインターフェース１５８との間で行われる各種データの授受を制御するとともに、メモリバス１５９を介して接続されたRAM１５３のメモリコントロールを行うようになされている。

【０１１４】またホストーPCIブリッジ１５４は、ビデオコントローラ１５６とAGP（Accelerated Graphics Port）に沿った信号線を介して接続されており、これによりホストーPCIブリッジ１５４およびビデオコントローラ１５６間で画像データを高速転送するようになされている。

【０１１５】ビデオキャプチャ処理チップ１８３は、シリアルバス１８２と接続されており、シリアルバス１８２を介してCCDカメラ１０７で撮像された画像データが供給されると、これを内蔵のフレームメモリ（図示せず）に一旦格納し、JPEG（Joint Photographic Experts Group）規格に従って画像圧縮処理を施すことによりJPEG画像データを生成した後、そのJPEG画像データを再度フレームメモリに格納するようになされている。

【０１１６】ビデオキャプチャ処理チップ１８３は、CPU１５０からの要求に応じて、フレームメモリに格納されているJPEG画像データを、バスマスタ機能を用いてRA

ＭＩ５３へ転送した後、JPEG画像データとしてハードディスクドライブ（HDD）１６７へ転送する。

【０１１７】ビデオコントローラ１５６は、逐次供給される各種アプリケーションソフトウェアに基づく画像データや、CCDカメラ１０７で撮像された画像データを表示部１０２の液晶ディスプレイ１０９に出力することにより、複数のウィンドウ画面を表示するようになされている。

【０１１８】IEEE1394インターフェース１５７は、IEEE1394端子１２８と直結されており、IEEE1394端子１２８を介して他の装置やデジタルビデオカメラなどの外部デバイスと接続するようになされている。

【０１１９】PCカードインターフェース１５８は、オプション機能を追加するときに適宜PCカードスロット１２７に装着されるPCカード（図示せず）と接続され、PCカードを介して、ドライブと接続するようになされ、必要に応じて、磁気ディスク、光ディスク、光磁気ディスク、または半導体メモリなどが装着される。

【０１２０】PCIバス１５５は、ISA（Industrial Standard Architecture）バス１６５とPCI－ISAブリッジ１６６を介して接続されており、PCI－ISAブリッジ１６６にはHDD１６７およびUSB端子１２１が接続されている。

【０１２１】ここでPCI－ISAブリッジ１６６は、IDE（Intelligent Drive Electronics）インターフェース、コンフィギュレーションレジスタ、RTC（Real Time Clock）回路およびUSBインターフェース等によって構成されており、クロックジェネレータ１６０から与えられるシステムクロックを基にIDEインターフェースを介してHDD１６７を制御する。

【０１２２】HDD１６７のハードディスクには、Windows（登録商標）９８などのOS（Operating System）、電子メールプログラム、オートパイロットプログラム、ジョグダイヤルサーバプログラム、ジョグダイヤルドライバ、キャプチャソフトウェア、およびこれら以外の各種アプリケーションソフトウェアが格納されており、起動処理の過程で逐次RAM１５３に転送されてロードされる。

【０１２３】PCI－ISAブリッジ１６６は、USB端子１２１を介して接続される図示せぬフレキシブルディスクドライブ、プリンタおよびUSBマウス等の外部デバイスを、USBインターフェースを介して制御するとともに、ISAバス１６５に接続されるモデム１６９およびサウンドコントローラ１７０を制御する。

【０１２４】モデム１６９は、モデム端子１２５から公衆回線網５を介してインターネットサービスプロバイダ６に接続し、さらにインターネットサービスプロバイダ６を介してインターネット７へダイヤルアップIP（Internet Protocol）接続するようになされている。

【０１２５】サウンドコントローラ１７０は、マイクロフォン１１３で集音された音声信号をデジタル変換することにより音声データを生成し、これをCPU１５０に出力するとともに、CPU１５０から供給される音声データをアナログ変換することにより音声信号を生成し、これを内蔵スピーカ１０５を介して外部に出力する。

【０１２６】またISAバス１６５には、I/O（In/Out）コントローラ１７３が接続されており、外部電源コネクタ１２２から電源供給充電制御回路１８５を介して外部電源の電力供給を受け、電源スイッチ１０６がオンされたときに各回路へ電力の供給を行う。なお、ここでもI/Oコントローラ１７３は、クロックジェネレータ１６０から供給されるシステムクロックを基に動作する。

【０１２７】また電源供給充電制御回路１８５は、I/Oコントローラ１７３によって制御され、バッテリコネクタ１２９に接続されたバッテリパック１３０の充電を制御する。

【０１２８】I/Oコントローラ１７３は、マイクロコントローラ、I/Oインターフェース、CPU，ROM，RAM等によって構成されており、フラッシュメモリ１７９に格納されているBIOS（Basic Input/Output System）に基づいてOSやアプリケーションソフトウェアと液晶ディスプレイ１０９やHDD１６７等の各種周辺機器との間におけるデータの入出力を制御する。また、I/Oコントローラ１７３は、赤外線ポート１１８と接続され、例えば他の装置との間で赤外線通信を実行するようになされている。

【０１２９】さらにI/Oコントローラ１７３は、反転スイッチ１７７と接続されており、撮像部１１１が液晶ディスプレイ１０９の背面側方向に１８０度回転されたとき、反転スイッチ１７７がオンされ、その旨をPCI－ISAブリッジ１６６およびホストーPCIブリッジ１５４を介してCPU１５０に通知する。

【０１３０】これに加えてI/Oコントローラ１７３は、全押し／半押しスイッチ１７８と接続されており、本体１０１の上面に設けられたシャッタボタン１０８が半押し状態にされたとき、全押し／半押しスイッチ１７８が半押し状態にオンされ、その旨をCPU１５０に通知するとともに、シャッタボタン１０８が全押し状態にされたとき、全押し／半押しスイッチ１７８が全押し状態にオンされ、その旨をCPU１５０に通知する。すなわち、CPU１５０は、HDD１６７のハードディスクからキャプチャソフトウェアをRAM１５３に立ち上げた状態で、ユーザによってシャッタボタン１０８が半押し状態にされると静止画像モードに入り、CCDカメラ１０７を制御して静止画像のフリーズを実行し、全押し状態にされるとフリーズされた静止画像データを取り込み、ビデオコントローラ１５６に出力する。

【０１３１】これに対してCPU１５０は、キャプチャソフトウェアを立ち上げない状態で、ユーザによってシャッタボタン１０８が全押し状態にされると動画像モードに入り、最大６０秒程度の動画像を取り込み、ビデオコントローラ１５６に出力する。

【０１３２】ところで、I/Oコントローラ１７３のROMには、ウェイクアッププログラム、キー入力監視プログラム、LED制御プログラム、およびジョグダイヤル状態監視プログラム、その他種々の制御プログラムが格納されている。

【０１３３】ジョグダイヤル状態監視プログラムは、HDD１６７のハードディスクに格納されているジョグダイヤルサーバプログラムと連動して用いられるプログラムであり、ジョグダイヤル１２４が回転操作または押圧操作されたか否かを監視するためのプログラムである。

【０１３４】ウェイクアッププログラムは、PCI－ISAブリッジ１６６内のRTC回路から供給される現在時刻が予め設定した開始時刻と一致すると、CPU１５０によって所定の処理を実行するように制御されたプログラムであり、キー入力監視プログラムは、操作キー１０３およびその他の各種キースイッチからの入力を監視するプログラムである。LED制御プログラムは、電源ランプPL、電池ランプBL、メッセージランプML等の各種ランプの点灯を制御するプログラムである。

【０１３５】またI/Oコントローラ１７３のRAMには、ジョグダイヤル状態監視プログラム用のI/Oレジスタ、ウェイクアッププログラム用の設定時刻レジスタ、キー入力監視プログラム用のキー入力レジスタ、LED制御プログラム用のLED制御レジスタおよびその他の各種プログラム用のレジスタが設けられている。

【０１３６】設定時刻レジスタは、ウェイクアッププログラムで用いるためにユーザが予め任意に設定した開始時刻の時間情報を格納するようになされている。従って、I/Oコントローラ１７３は、ウェイクアッププログラムに基づいてRTC回路から供給される現在時刻が任意に設定した開始時刻と一致するか否かを判定し、開始時刻と一致したときには、その旨をCPU１５０に通知する。これにより、CPU１５０は、開始時刻で予め設定された所定のアプリケーションソフトウェアを立ち上げ、そのアプリケーションソフトウェアに従って、所定の処理を実行する。

【０１３７】またキー入力監視レジスタは、操作キー１０３、スティック１０４、左クリックボタン１０４Ａ、右クリックボタン１０４Ｂ、およびセンタボタン１０５Ｃ等の入力操作に応じた操作キーフラグを格納するようになされている。

【０１３８】従ってI/Oコントローラ１７３は、キー入力監視プログラムに基づいて、例えば、スティック１０４によるポインティング操作や、左クリックボタン１０４Ａ、右クリックボタン１０４Ｂ、およびセンタボタン１０４Ｃのクリック操作が行われたか否かを操作キーフラグの状態に基づいて判定し、ポインティング操作やクリック操作が行われたときには、その旨をCPU１５０に通知する。

【０１３９】ここでポインティング操作とは、スティック１０４を指で上下左右に押圧操作することによりマウスカーソルを画面上の所望位置に移動する操作のことであり、クリック操作とは左クリックボタン１０４Ａまたは右クリックボタン１０４Ｂを指で素早く押して離す操作のことである。

【０１４０】これによりCPU１５０は、ポインティング操作によるマウスカーソルの移動やクリック操作に応じた所定の処理を実行する。

【０１４１】またLED制御レジスタは、電源ランプPL、電池ランプBL、メッセージランプML等の各種ランプの点灯状態を示す点灯フラグを格納するようになされている。

【０１４２】従ってI/Oコントローラ１７３は、例えば、ジョグダイヤル１２４の押圧操作によりCPU１５０がHDD１６７のハードディスクから電子メールプログラムを立ち上げ、その電子メールプログラムに従って電子メールを受け取ったときに点灯フラグを格納するとともに、その点灯フラグに基づいてLED１８１を制御することによりメッセージランプMLを点灯させる。

【０１４３】またジョグダイヤル状態監視プログラム用のI/Oレジスタは、ジョグダイヤル１２４に対する回転操作および押圧操作に応じた回転操作フラグおよび押圧操作フラグを格納するようになされている。

【０１４４】従ってI/Oコントローラ１７３は、回転検出部１８８を介して接続されたジョグダイヤル１２４の回転操作および押圧操作により複数のメニュー項目の中からユーザが所望するメニュー項目が選択されたとき、I/Oレジスタに格納されている回転操作フラグおよび押圧操作フラグを立てるとともに、その旨をCPU１５０に通知する。

【０１４５】これによりCPU１５０は、HDD１６７から読み出してRAM１５３上に立ち上げたジョグダイヤルサーバプログラムに従って、ジョグダイヤル１２４の回転操作および押圧操作によって決定されたメニュー項目に対応するアプリケーションソフトウェアを立ち上げて所定の処理を実行する。

【０１４６】ここでI/Oコントローラ１７３は、電源スイッチ１０６がオフでOSが起動していない状態であっても、電源供給充電制御回路１８５の制御によって常時動作しており、専用キーを設けることなく省電力状態または電源オフ時のジョグダイヤル１２４の押圧操作によってユーザが所望するアプリケーションソフトウェアやスクリプトファイルを起動するようになされている。

【０１４７】なお、I/Oコントローラ１７３は、シリアルバス１８２とも接続されており、操作キー１０３やジョグダイヤル１２４によって設定されたCCDカメラ１０７に対する各種設定パラメータをシリアルバス１８２を介して供給することにより、CCDカメラ１０７における明るさやコントラストを調整するようになされている。

【０１４８】図１１は、チケットレス端末３の機能を説

明するブロック図である。

【０１４９】入出力管理プログラム１９１は、操作キー１０３、スティック式ポインティングディバイス１０４、もしくはジョグダイヤル１２４を用いて、ユーザが入力した操作または命令を示す信号を、対応するアプリケーションに供給したり、各種アプリケーションの処理に基づいて、所定のデータをIEEE1394端子１２８もしくはUSB端子１２１に出力して他の機器に送信させたり、CCDカメラ１０７で撮像された画像データを液晶ディスプレイ１０９に出力して画像を表示させる処理を管理するプログラムである。

【０１５０】サイバーコードファインダ（CyberCode Finder）（商標）１９２は、入出力管理プログラム１９１の処理によりユーザの操作に対応する信号、または他の機器から送信されてきた指令（コマンド）に対応する信号の供給を受け、その信号を基に、液晶ディスプレイ１０９に、所定の画面を表示させ、CCDカメラ１０７により画像を撮像する処理を実行するとともに、撮像された画像からサイバーコードのコード番号を認識する処理を実行するためのプログラムである。

【０１５１】認証プログラム１９３は、サイバーコードファインダ１９２の処理により認識されたサイバーコードのコード番号を基に、IEEE1394端子１２８もしくはUSB端子１２１を介して、サイバーコード認証サイト８にアクセスし、ユーザ認証の実行を要求し、サイバーコード認証サイト８から供給された認証結果を、液晶ディスプレイ１０９に表示させるためのプログラムである。

【０１５２】図１２は、サイバーコード生成プログラム発行／認証サーバ１１の電気的内部の構成例を示す図である。

【０１５３】CPU２０１は、ROM２０２またはハードディスク装置２０４に記憶されているプログラムに従って、各種処理を実行するようになされている。ROM２０２は、例えば、起動時に実行されるプログラムや各種のデータを記憶している。RAM２０３は、CPU２０１により各種の処理が実行されるとき必要なデータやプログラムを記憶する。ハードディスク装置２０４は、このサイバーコード生成プログラム発行／認証サーバ１１をサーバとして機能させるサーバプログラムや、図１３を用いて後述する各種のプログラムを記憶している。

【０１５４】表示部２０５は、LCDもしくはCRT（Cathode Ray Tube）などからなり、CPU２０１より供給される画像データに対応する画像を表示するようになされている。入力部２０６は、キーボード、ボタン、スイッチもしくはマウスなどからなり、CPU２０１に各種の指令を入力するとき、サイバーコード生成プログラム発行／認証サーバ１１の管理者により操作される。

【０１５５】ネットワークインターフェース２０７は、インターネット７に接続され、サイバーコード生成プログラム発行／認証サーバ１１宛のIPパケットを受信するとともに、CPU２０１より供給されたデータから、インターネットプロトコルに従ってIPパケットを生成し、インターネット７に出力する。

【０１５６】ドライブ２０８には、必要に応じて、磁気ディスク２１１、光ディスク２１２、光磁気ディスク２１３、または半導体メモリ２１４などが装着され、CPU２０１が実行するプログラムなどがインストールされる。

【０１５７】図１３は、サイバーコード生成プログラム発行／認証サーバ１１の機能を説明するブロック図である。

【０１５８】入出力管理プログラム２２１は、入力部２０６を用いて、ユーザが入力した操作または命令を示す信号もしくはネットワークインターフェース２０７から入力される信号を、対応するアプリケーションに供給したり、各種アプリケーションの処理に基づいて、所定のデータをネットワークインターフェース２０７に出力して他の機器に送信させたり、所定の画像データを表示部２０５に出力して画像を表示させる処理を管理するプログラムである。

【０１５９】Seed作成プログラム２２２は、入出力管理プログラム２２１の処理により他の機器から送信されてきた指令（サイバーコード生成プログラムの発行要求）に対応する信号の供給を受け、その信号を基に、ユーザIDを生成（発行）し、さらに次式（１）に従って、乱数発生用SeedIDを作成する。

$$SeedID = f\ (UID, TID) \quad \cdots (1)$$

【０１６０】上記式（１）において、UIDは、例えば、携帯電話機１のユーザ毎に割り当てられる固有のユーザIDを表わし、TIDは、サイバーコード生成プログラムの発行要求を受信した時刻（すなわち、サイバーコード生成プログラム発行開始時刻）を表わす。作成された乱数発生用SeedIDは、後述するように、サイバーコード生成プログラムを作成するときに利用される。

【０１６１】ここで乱数(random numbers)について説明する。乱数とは、一般に数の集合から、無作為抽出で抜き出された数を示すものであり、真性乱数、物理乱数、および擬似乱数(pseudo random number)がある。

【０１６２】真性乱数は、ビット列にすると、０と１の発生確率がそれぞれ１／２で、各ビットは他の部分と独立なiid（independent and identically distributed）である。

【０１６３】物理乱数は、量子力学の効果を増幅してディジタル化したものであり、平滑化して０および１のバランスをとれば、真性乱数になるものである。

【０１６４】疑似乱数は、種(seed)と呼ばれる入力ビットパタンを基に計算された、種よりも長いランダムに見えるビット・パタンであり、髭と周期がある。なお、擬似乱数は、決定的（deterministic）アルゴリズムから

生成されるので、種が決まれば出力乱数は一意に決まるため、暗号に使う時には、種を秘密にする必要がある。Seed作成プログラム２２２は、この擬似乱数を使用する。すなわち、作成されるサイバーコード生成プログラムには、この擬似乱数が使用され、基となる種はSeed作成プログラム２２２により生成される。

【０１６５】図１３の説明に戻る。サイバーコード生成プログラム発行部２２３は、入出力管理プログラム２２１の処理により他の機器から送信されてきた指令（サイバーコード生成プログラムの発行要求）に対応する信号の供給を受けてSeed作成プログラム２２２の処理により作成された乱数発生用SeedID、発行要求のあった携帯電話機１のユーザを表わすユーザID（UID）、および、サイバーコード生成プログラム発行開始時刻TIDを基に、例えば、

P(UID, TID, SeedID)(t)

で表わされるようなユーザ毎に固有のサイバーコード生成プログラムPID（Java（登録商標）アプレット）を作成する。

【０１６６】サイバーコード生成プログラム発行／認証サーバ１１は、このユーザ毎に固有のアルゴリズムを持ったプログラムを、ユーザに配布することにより、アルゴリズム自体を認証キーとして利用することができる。

【０１６７】サイバーコード生成プログラム発行部２２３は、作成されたユーザ毎に固有のサイバーコード生成プログラムPIDを、インターネット７、インターネットサービスプロバイダ６、公衆回線網５、基地局２を介して、発行要求のあった携帯電話機１に送信する。

【０１６８】認証用キー分離プログラム２２４は、入出力管理プログラム２２１の処理により他の機器から送信されてきた指令（サイバーコード生成プログラムの実行により生成されたサイバーコードのコード番号）に対応する信号の供給を受け、コード番号に含まれるユーザIDを分離する。例えば、８桁で表わされるコード番号のうち、下４桁がユーザIDとして埋め込まれている場合、上４桁と下４桁のコード番号に分離される。

【０１６９】認証プログラム２２５は、入出力管理プログラム２２１の処理によりチケットレス端末３から送信されてきた指令（サイバーコード生成プログラムの実行により生成されたサイバーコードのコード番号）に対応する信号の供給を受けて認証用キー分離プログラム２２４の処理により分離されたユーザIDを基に、登録ユーザ情報データベース１２から、対応するユーザIDの発行開始時刻TIDおよび乱数発生用SeedIDを検索する。

【０１７０】認証プログラム２２５は、ユーザID、検索された開始時刻TIDおよび乱数発生用Seedから、サイバーコード生成プログラムPIDを作成し、コード番号受信時刻を基にそのプログラムを実行する。認証プログラム２２５は、サイバーコード生成プログラムPIDの実行により生成されたサイバーコードのコードパターンから得られるコード番号と、受信したコード番号とを比較し、一致すれば認証に成功した旨を、入出力管理プログラム２２１、ネットワークインターフェース２０７、およびインターネット７を介してチケットレス端末３に送信する。なお、認証に失敗した場合にも、その旨が同様に送信される。

【０１７１】次に、図１４を参照して、本発明に係るサイバーコードについて説明する。

【０１７２】サイバーコードは、図１４に示されるように、ロゴマーク部２３１とコード部２３２から構成されており、これらロゴマーク部２３１とコード部２３２の全体は、例えば、１個の正方形状のセルの矩形領域を１ブロックと表現すると、縦方向が９．５ブロックの長さで、横方向が７ブロック分の長さの長方形の領域内に配置されている。

【０１７３】ロゴマーク部２３１は、ロゴマーク、文字、または数字など、サイバーコードに関連する白抜きの可読文字情報が表示されている。ここで、例えば、ロゴマークとしては、サイバーコードのコード体系に付された「CyberCode」など、何を意味するコードなのかを、人間が判読可能なマークとして、白抜き文字で表示される。

【０１７４】コード部２３２は、７×７の全４９個のブロック（またはセル）がマトリクス状に配置されたマトリクス構造を有し、１つのサイバーコードで２４ビットの情報をコード化し得るように構成されている。具体的には、四隅のブロック（コーナセル）およびその周囲の３ブロックを含む全１６ブロック（１６ビット）はデータを構成せず、また残り３３ブロック（３３ビット）中、９ブロック（９ビット）は、コードデータが正しいコードデータであることを確かめるためのチェックデータを構成する。従って、コード部２３２には、２４ビットのビットコードで表わされるサイバーコードの識別番号（コード番号）が設定される。

【０１７５】コード部２３２は、７×７の全４９個のブロックで構成させる以外に、８×８の全６４個のブロック（またはセル）で構成させるようにしてもよい。これにより、より多くの情報をコード化することが可能になる。

【０１７６】ID部２３３は、コード部２３２においてコード化された２４ビットのデータを１６進数で表わしたものであり、サイバーコードとして必須の部位ではない。

【０１７７】なお、サイバーコードの詳細については、特開２０００－８２１０８号および特開２０００－１４８９０４号公報に開示されている。

【０１７８】次に、図１５のフローチャートを参照して、携帯電話機１が、認証サイト８にアクセスし、コンサート会場４に入場するための入場チケットの代替となるサイバーコード（認証キー）を生成するためのサイバ

ーコード生成プログラムをダウンロードする処理について説明する。

【０１７９】ステップＳ１において、携帯電話機１の入出力制御プログラム８１は、操作キー４１もしくはジョグダイヤル４４を用いてユーザが入力した操作を示す信号を表示プログラム８３に供給し、例えば、図１６に示されるようなメニュー画面を液晶ディスプレイ３５に表示させる。

【０１８０】図１６に示すメニュー画面には、ユーザが選択可能な、「メール」、「ダウンロード」、および「Java（登録商標）アプレット」などの項目が表示されている。ユーザが、操作キー４１もしくはジョグダイヤル４４を用いて、「ダウンロード」の項目を選択すると、入出力制御プログラム８１は、ユーザが入力した操作を示す信号をウェブブラウザ８２に供給する。

【０１８１】ウェブブラウザ８２は、データ通信プログラム８７に対して、アンテナ３１、基地局２、公衆回線網５、インターネットサービスプロバイダ６、およびインターネット７を介して、サイバーコード認証サイト８のサイバーコード生成プログラム発行／認証サーバ１１との通信を実行させる。

【０１８２】ステップＳ１１において、サイバーコード認証サイト８のサイバーコード生成プログラム発行／認証サーバ１１は、所定の通信処理を実行し、通信が確立した旨を、インターネット７、インターネットサービスプロバイダ６、公衆回線網５、および基地局２を介して、携帯電話機１に通知（送信）する。このとき、サーバのトップページに対応するコンパクトHTMLファイルも携帯電話機１に送信される。

【０１８３】ステップＳ２において、携帯電話機１のデータ通信プログラム８７は、アンテナ３１を介して、サイバーコード生成プログラム発行／認証サーバ１１より、通信確立の通知を受け、さらに、受信したコンパクトHTMLファイルを表示プログラム８３に供給し、例えば、図１７に示されるようなダウンロード画面（トップページ）を液晶ディスプレイ３５に表示させる。

【０１８４】図１７に示すダウンロード画面には、ユーザが選択可能な、「認証用サイバーチケット」、および「認証用貨幣」などの項目が表示されている。ユーザが、操作キー４１もしくはジョグダイヤル４４を用いて、「認証用サイバーチケット」の項目を選択すると、入出力制御プログラム８１は、ユーザが入力した操作を示す信号をウェブブラウザ８２に供給する。

【０１８５】ウェブブラウザ８２は、データ通信プログラム８７に対して、アンテナ３１、基地局２、公衆回線網５、インターネットサービスプロバイダ６、およびインターネット７を介して、サイバーコード認証サイト８のサイバーコード生成プログラム発行／認証サーバ１１に、ユーザが入力した操作を示す信号を送信させ、サイバーコード生成プログラム発行／認証サーバ１１から対応するHTMLファイルを受信させ、表示プログラム８３に供給させる。

【０１８６】表示プログラム８３は、供給されたHTMLファイルを基に、例えば、図１８に示されるようなサイバーチケットダウンロード画面を液晶ディスプレイ３５に表示させる。

【０１８７】図１８に示すサイバーチケットダウンロード画面には、ユーザが選択可能（ダウンロード可能）な、「△×試合」、「×○映画入場」、「○△コンサート」、「×□試合」、および「□○コンサート」の項目が表示されている。ユーザが、操作キー４１もしくはジョグダイヤル４４を用いて、「○△コンサート」の項目を選択すると、入出力制御プログラム８１は、ユーザが入力した操作を示す信号をウェブブラウザ８２に供給する。

【０１８８】ウェブブラウザ８２は、表示プログラム８３に対して、例えば、図１９に示されるようなユーザ登録画面を液晶ディスプレイ３５に表示させる。

【０１８９】図１９に示すユーザ登録画面には、「○△コンサート認証用サイバーチケットをダウンロードするためのユーザIDを登録しますか？」といったメッセージとともに、その選択を促す「Yes」および「No」の項目を表示させる。ユーザが、操作キー４１もしくはジョグダイヤル４４を用いて、「Yes」の項目を選択すると、入出力制御プログラム８１は、ユーザが入力した操作を示す信号をウェブブラウザ８２に供給する。

【０１９０】ウェブブラウザ８２は、データ通信プログラム８７に対して、アンテナ３１、基地局２、公衆回線網５、インターネットサービスプロバイダ６、およびインターネット７を介して、サイバーコード認証サイト８のサイバーコード生成プログラム発行／認証サーバ１１に、ユーザが入力した操作を示す信号を送信させる。これにより、サイバーコード生成プログラム発行／認証サーバ１１に対して、サイバーコード生成プログラムの発行が要求される。

【０１９１】ステップＳ１２において、サイバーコード生成プログラム発行／認証サーバ１１の入出力管理プログラム２２１は、携帯電話機１から、ネットワークインターフェース２０７を介してサイバーコード生成プログラムの発行要求を受けて、その要求を示す信号をSeed作成プログラム２２２に供給し、乱数発生用SeedIDを作成させる。

【０１９２】Seed作成プログラム２２２は、サイバーコード生成プログラムの発行要求を受信した現在時刻TIDを取得し、その時刻TIDを基に、ユーザ毎に固有のユーザIDを生成するとともに、生成されたユーザIDおよび時刻TIDを基に、上記式（１）に従って、乱数発生用SeedIDを作成する。

【０１９３】ステップＳ１３において、サイバーコード生成プログラム発行部２２３は、ステップＳ１２の処理

で作成された乱数発生用SeedID、ユーザID、および時刻TIDを基に、サイバーコード生成プログラムPIDを作成する。ここで作成されるサイバーコード生成プログラムPIDは、そのプログラムが実行されることにより生成されるサイバーコードのコード番号（ID部２３３）の下４桁に、ユーザIDが埋め込まれるようになされている。すなわち、認証時に、ユーザIDが必要とされるため、コード番号にユーザIDが埋め込まれるようになされている。

【０１９４】ステップＳ１４において、サイバーコード生成プログラム発行部２２３は、サイバーコード生成プログラムPIDの作成に成功したか否かを判定し、サイバーコード生成プログラムPIDの作成に成功したと判定した場合、ステップＳ１５に進み、生成されたユーザIDに対応付けて、サイバーコード生成プログラム発行開始時刻TIDおよび乱数発生用SeedIDを、登録ユーザ情報データベース１２に記録させる。

【０１９５】ステップＳ１６において、サイバーコード生成プログラム発行部２２３は、ステップＳ１３の処理で作成されたサイバーコード生成プログラムPIDを、入出力管理プログラム２２１、ネットワークインターフェース２０７、インターネット７、インターネットサービスプロバイダ６、公衆回線網５、および基地局２を介して、携帯電話機１に送信する。

【０１９６】これに対して、ステップＳ１４において、システムエラーなどによりサイバーコード生成プログラムPIDの作成に成功しなかった、すなわち、サイバーコード生成プログラムPIDの作成に失敗したと判定された場合、ステップＳ１７に進み、サイバーコード生成プログラム発行部２２３は、サイバーコード生成プログラムの作成に失敗した旨を、入出力管理プログラム２２１、ネットワークインターフェース２０７、インターネット７、インターネットサービスプロバイダ６、公衆回線網５、および基地局２を介して、携帯電話機１に送信する。

【０１９７】ステップＳ３において、携帯電話機１のデータ通信プログラム８７は、アンテナ３１を介して、サイバーコード生成プログラム発行／認証サーバ１１からサイバーコード生成プログラムの作成失敗の通知を受信したか否かを判定し、サイバーコード生成プログラムの作成失敗の通知を受信したと判定した場合、ステップＳ４に進み、受信したサイバーコード生成プログラムの作成失敗の通知を示す信号を表示プログラム８３に供給する。表示プログラム８３は、供給された信号に基づいて、例えば、「サイバーコード生成プログラムのダウンロードに失敗しました」といったエラーメッセージを液晶ディスプレイ３５に表示させる。

【０１９８】ステップＳ３において、サイバーコード生成プログラムの作成失敗の通知を受信していないと判定された場合、ステップＳ５に進み、携帯電話機１のデータ通信プログラム８７は、アンテナ３１を介して、サイバーコード生成プログラム発行／認証サーバ１１から送信されてきたサイバーコード生成プログラムPIDを受信し、それをJava（登録商標）アプレット９１としてメモリ８６に記録させる。

【０１９９】ステップＳ４もしくはステップＳ５の処理の後、ステップＳ６において、ウェブブラウザ８２は、データ通信プログラム８７に対して、サイバーコード生成プログラム発行／認証サーバ１１との通信を解除させ、処理は終了される。

【０２００】以上の処理により、携帯電話機１は、ユーザ毎に固有のサイバーコード生成プログラムPIDを取得することができ、図２０を用いて後述する、サイバーコード生成プログラムの実行により生成されるサイバーコードを認証キーとして利用することができる。

【０２０１】次に、図２０のフローチャートを参照して、携帯電話機１のユーザが、上述した処理によって取得（ダウンロード）したサイバーコード生成プログラムPIDを実行して、コンサート会場４で開催されるコンサートの入場チケットの代替となるサイバーコードを生成し、そのサイバーコードをチケットレス端末３で認識させ、認識されたコード番号を、サイバーコード認証サイト８で認証させる処理について説明する。

【０２０２】携帯電話機１のユーザは、操作キー４１もしくはジョグダイヤル４４を用いて、図１６に示したようなメニュー画面を液晶ディスプレイ３５に表示させ、「Java（登録商標）アプレット」の項目を選択する。これにより、ステップＳ３１において、Java（登録商標）アプレット実行プログラム８５は、ユーザが入力した操作を示す信号を表示プログラム８３に供給し、図２１に示されるようなJava（登録商標）アプレット実行画面を液晶ディスプレイ３５に表示させる。

【０２０３】図２１に示すJava（登録商標）アプレット実行画面には、ユーザによってダウンロードされた、「○△コンサート」、および「×○映画入場」などのJava（登録商標）アプレット（サイバーコード生成プログラムPID）の項目が表示されている。ユーザが、操作キー４１もしくはジョグダイヤル４４を用いて、「○△コンサート」の項目を選択すると、Java（登録商標）アプレット実行プログラム８５は、選択された「○△コンサート」に対応するサイバーコード生成プログラムPIDを実行する。

【０２０４】ステップＳ３２において、Java（登録商標）アプレット実行プログラム８５は、現在時刻Tuを基に、サイバーコードを生成し、生成されたサイバーコードを液晶ディスプレイ３５に表示させる。これにより、例えば、図２２に示されるように、「○△コンサート認証用サイバーチケット」といったサイバーコードの内容を示す情報および現在時刻とともに、生成されたサイバーコード（認証用サイバーチケット）２４１が表示される。

【０２０５】ところで、サイバーコード生成プログラムPIDが実行されると、現在時刻を基にサイバーコード２４１が生成されるが、このサイバーコード２４１は、図２３に示されるように、所定の時間（例えば、１０秒）毎に更新（変化）される。

【０２０６】図２３の例の場合、時刻ｔ１を基にサイバーコード２４１－１が生成され、時刻ｔ２を基にサイバーコード２４１－２が生成され、時刻ｔ３を基にサイバーコード２４１－３が生成され、時刻ｔ４を基にサイバーコード２４１－４が生成され、同様に、所定の時間毎にサイバーコード２４１が生成される。

【０２０７】すなわち、携帯電話機１でサイバーコードが生成されてから、そのコードパターンがチケットレス端末３で認識されることにより得られるコード番号がサイバーコード認証サイト８に送信され、サイバーコード認証サイト８でコード番号に含まれるユーザIDが分離され、分離されたユーザIDを基に、乱数発生用SeedIDが作成され、作成された乱数発生用SeedID、ユーザID、およびコード番号受信時刻からサイバーコード生成プログラムPIDが再度作成され、そのプログラムを実行することによって生成されるサイバーコードは、携帯電話機１で作成されたサイバーコードと同一時刻に作成されたものであるとして保証するようになされている。

【０２０８】図２３の例においては、時刻ｔ３を基にサイバーコード２４１－２が生成され、時刻ｔａでサイバーコード２４１－２が認識され、認識されたコードパターンから得られるコード番号がサイバーコード認証サイト８に送信され、サイバーコード認証サイト８において、時刻ｔｂを基に生成されるサイバーコード２４２とは同一のものであるとすることができる。

【０２０９】このように、携帯電話機１でサイバーコード生成プログラムPIDが実行される時刻Tuと、サイバーコード認証サイト８で再度サイバーコード生成プログラムPIDが作成され、そのプログラムが実行される時刻tsは、同一時刻であるものとすることができる。すなわち、所定の時間内に同一のサイバーコード生成プログラムPIDが実行され、サイバーコードが生成されたとして認証される。なお、サイバーコード２４１が生成される時間間隔を短くすることによって、生成されたサイバーコードの有効期限が短くなり、コードの盗用による認証性が減少するため、認証精度を向上させることができる。

【０２１０】図２０の説明に戻る。ステップＳ３３において、携帯電話機１のユーザは、液晶ディスプレイ３５に表示されているサイバーコード２４１を、チケットレス端末３のCCDカメラ１０７にかざし、サイバーコード２４１が撮像されるようにその位置を調整する。

【０２１１】このとき、チケットレス端末３では、予めサイバーコードファインダ１９２が起動されており、液晶ディスプレイ１０９に、例えば、図２４に示されるような画面が表示されている。

【０２１２】ステップＳ４１において、チケットレス端末３のサイバーコードファインダ１９２は、CCD１０７により画像を撮像する処理を実行させるとともに、撮像された画像からサイバーコードを認識する処理を実行する。このとき、液晶ディスプレイ１０９に表示されている画面は、例えば、図２５に示されるように、「認証中」といったメッセージを表示させ、ユーザに対して、サイバーコードの認証中である旨を知らしめる。

【０２１３】サイバーコードファインダ１９２は、撮像された画像からサイバーコードのコードパターンから得られるコード番号を認識する。ステップＳ４２において、認証プログラム１９３は、認識されたコード番号をサイバーコード認証サイト８に送信し、ユーザ認証の実行を要求する。

【０２１４】ステップＳ５１において、サイバーコード認証サイト８のサイバーコード生成プログラム発行／認証サーバ１１は、チケットレス端末３から送信されてきたコード番号を受信し、ユーザ認証の要求を受ける。ステップＳ５２において、サイバーコード生成プログラム発行／認証サーバ１１の認証用キー分離プログラム２２４は、ステップＳ５１の処理で受信されたコード番号から、ユーザIDを分離する。

【０２１５】ステップＳ５３において、認証プログラム２２５は、ステップＳ５２の処理で分離されたユーザIDを基に、登録ユーザ情報データベース１２から、対応するユーザIDの発行開始時刻TIDおよび乱数発生用SeedIDを検索する。ステップＳ５４において、認証プログラム２２５は、ステップＳ５２の処理で分離されたユーザID、ステップＳ５３の処理で検索された時刻TIDおよび乱数発生用SeedIDから、サイバーコード生成プログラムPIDを再度作成する。

【０２１６】ステップＳ５５において、認証プログラム２２５は、コード番号受信時刻を基に、ステップＳ５４の処理で作成されたサイバーコード生成プログラムPIDを実行し、サイバーコード２４２を生成する。ステップＳ５６において、認証プログラム２２５は、ステップＳ５５の処理により生成されたサイバーコード２４２のコードパターンから得られるコード番号と、ステップＳ５１の処理で受信したコード番号から、一方向性マッチング（認証処理）を行う。

【０２１７】認証処理としては、サイバーコードのコード番号の有効期限が切れていないか（例えば、以前に開催されたコンサートの認証用サイバーチケットがコピーされたものであり、コンサート開催日を過ぎていないか）、もしくは、認証されたサイバーコードが、所定のユーザID、時刻TID、および乱数発生用SeedIDから作成されたものではないか（例えば、別のサイバーコード生成プログラムPIDにより作成されたものであるか）などを判定する。

【０２１８】ステップＳ５７において、認証プログラム２２５は、認証結果を、入出力管理プログラム２２１、ネットワークインターフェース２０７、およびインターネット７を介してチケットレス端末３に送信する。

【０２１９】ステップＳ４３において、チケットレス端末３の認証プログラム１９３は、サイバーコード認証サイト８から供給された認証結果を、液晶ディスプレイ１０９に表示させる。これにより、例えば、図２６に示されるように、「認証に成功しました！」といったメッセージが表示される。

【０２２０】以上のように、サイバーコード認証サイト８は、サイバーコード発行要求のあった携帯電話機１のユーザのユーザID、サイバーコード生成プログラム発行要求を受信した時刻TID、および乱数発生用SeedIDから、サイバーコード発生プログラムPIDを作成し、作成されたプログラムを要求元のユーザに配布するとともに、それらの情報を登録ユーザ情報データベース１２に記録させておく。そして、サイバーコード認証サイト８は、認証時に、チケットレス端末３から送信されてくるコード番号に含まれるユーザIDを基に、登録情報データベース１２から対応する時刻TIDおよび乱数発生用SeedIDを取得して、再びサイバーコード生成プログラムPIDを作成し（すなわち、認証しようとするユーザと同一のサイバーコード生成プログラムPIDを作成し）、サイバーコードを生成し、それを認証するようにしたので、サイバーコード生成プログラム自体に認証キーの機能を持たせることができる。

【０２２１】また、時刻を基にサイバーコードが生成されるため、認証時において唯一のサイバーコードであるという有効期限付きの認証キーとして利用することが可能になる。

【０２２２】また、サイバーコードのコード番号の下４桁に、ユーザIDを埋め込むようにして説明したが、本発明はこれに限られるものではなく、例えば、図２７（Ａ）に示されるように、サイバーコード２４１のビットパターンの一部（例えば、ブロック２５１－１および２５１－２）がユーザIDとして埋め込まれるか、図２７（Ｂ）に示されるように、複数毎のサイバーコード２４１－１乃至２４１－４が時系列的に配置され、それらのコードで１つのコード番号が表わされるようにして、その１枚（例えば、サイバーコード２４１－３）がユーザIDとして埋め込まれるか、もしくは、図２７（Ｃ）に示されるように、複数毎のサイバーコード２４１－１乃至２４１－４が空間的に配置され、それらのコードで１つのコード番号が表わされるようにして、その１枚（例えば、サイバーコード２４１－２）がユーザIDとして埋め込まれるようにしてもよい。

【０２２３】また、以上説明したチケットレスシステムにおいては、ｉ－アプリの制約に基づく問題点を解消することも可能である。すなわち、ｉ－アプリにおいては、一般的に以下のような制約があることが知られている。

（１）iアプリでは、セキュリティ保護のため、プログラム内部の処理を用いて、そのプログラムのダウンロード元のサイトにしか、アクセスすることができない。

（２）また、セキュリティ保護のため、プログラム内部の処理により、任意の場所（サイト）に電話をかけて通信を確立することは許可されていない。

【０２２４】従って、Java（登録商標）アプレットを用いて携帯電話機が認証のために、所定の認証サーバに通信するとなると、Java（登録商標）アプレット発行サーバと認証サーバが同一である必要がある。

【０２２５】また、ユーザ毎に唯一の認証プログラムを有するようにするためには、全てのイベントを一括して行うような認証サーバを構成する必要がある。

【０２２６】これに対して、本発明のチケットレスシステムによれば、サイバーコード生成プログラム（Java（登録商標）アプレット）がダウンロードされた携帯電話機１がサイバーコード生成プログラム発行／認証サーバ１１に通信するのではなく、チケットレス端末３がサイバーコード生成プログラム発行／認証サーバ１１に通信するため、アクセス先の制限を受けることがなくなる。

【０２２７】また、イベント毎にサイバーコード生成プログラム発行／認証サーバ１１を設けることが可能となり、ユーザは、ユーザ毎に唯一のサイバーコード生成プログラムをダウンロードすることができるとともに、イベント毎に異なる認証サーバにアクセスすることができる。

【０２２８】また、チケットレス端末３で携帯電話機１の液晶ディスプレイ３５に表示されたサイバーコード２４１が認識され、インターネット７などのネットワークを介してサイバーコード認証サイト８のサイバーコード生成プログラム発行／認証サーバ１１でユーザ認証を行うものとして説明したが、本発明はこれに限られるものではなく、チケットレス端末３とサイバーコード生成プログラム発行／認証サーバ１１を１つの装置として構成することも可能である。

【０２２９】さらに、携帯電話機１にサイバーコード生成プログラムをダウンロードし、そのプログラムを実行してサイバーコードを表示させるものとして説明したが、本発明はこれに限られるものではなく、例えば、表示機能を有し、かつ、サイバーコード生成プログラム（Java（登録商標）アプレット）が実行可能な携帯型パーソナルコンピュータ、ポータブルデバイス、PDA（Personal Digital Assistant）、もしくはPHS（Personal Handyphone System）などの装置全般に広く適用することができる。

【０２３０】また、以上においては、サイバーコード生成プログラム自体が認証キーとしての機能を持っている

ため、そのプログラムの実行により生成されるものは、サイバーコードの他、数字の配列、音声、もしくは絵柄などでもよい。

【０２３１】また、以上においては、携帯電話機１の液晶ディスプレイ３５に表示されるサイバーコードを認証用サイバーチケットとして利用するものとしたが、例えば、図１７に示したダウンロード画面において、ユーザによって、「認証用貨幣」の項目が選択された場合、ユーザが取引している所定の銀行にアクセスされ、ユーザの口座から所定金額の代替になる認証用貨幣コインを生成するためのサイバーコード生成プログラムがダウンロードされるようにしてもよい。この場合、ユーザが、所望の物品を購入する際に、サイバコード認識可能な自動販売機や店頭端末において、ユーザが携帯電話機１の液晶ディスプレイ３５に認証用貨幣（サイバーコード）を表示させ、上述したようにして認証されると、電子決済が実行される。

【０２３２】さらにまた、以上においては、様々なサイバーコード生成プログラム（Java（登録商標）アプレット）が携帯電話機１にダウンロードされることにより、メモリ８６の記憶容量が一杯になってしまうため、例えば、有効期限を過ぎた（既にコンサートが終了している）認証用サイバーチケットを自動消滅させるようにしたり、もしくは、図２１に示したJava（登録商標）アプレット実行画面において、ユーザによって、有効期限を過ぎたJava（登録商標）アプレットが選択された場合、「有効期限が過ぎているため、プログラムを実行することができません」といった警告メッセージを液晶ディスプレイ３５に表示させるようにしてもよい。

【０２３３】コンピュータにインストールされ、コンピュータによって実行可能な状態とされるプログラムを記録する記録媒体は、図１２に示すように、磁気ディスク２１１（フレキシブルディスクを含む）、光ディスク２１２（CD-ROM(Compact Disc-Read Only Memory)、DVD(Digital Versatile Disc)を含む）、光磁気ディスク２１３（MD(Mini-Disc)（登録商標）を含む）、もしくは半導体メモリ２１４などよりなるパッケージメディア、または、プログラムが一時的もしくは永続的に格納されるFlash ROMや、ハードディスクなどにより構成される。記録媒体へのプログラムの記録は、必要に応じてルータ、モデムなどのインターフェースを介して、公衆回線網５、ローカルエリアネットワークまたはインターネット７、デジタル衛星放送といった、有線または無線の通信媒体を利用して行われる。

【０２３４】なお、本明細書において、記録媒体に記録されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【０２３５】また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【０２３６】

【発明の効果】本発明の情報提供装置および方法、並びに第１のプログラムによれば、情報処理装置から送信されてくるプログラムの発行要求を受けて、情報処理装置に対して、ユーザIDを発行し、発行されたユーザID、および発行要求の受信時刻を基に、乱数を発生し、発生された乱数、ユーザID、および受信時刻を基に、所定画像を生成するためのプログラムを作成し、作成されたプログラムを情報処理装置に提供するようにしたので、プログラムを認証キーとして機能させることができる。

【０２３７】また本発明の情報処理装置および方法、並びに第２のプログラムによれば、情報提供装置に対してプログラムの送信を要求し、情報提供装置から提供されるプログラムを受信し、受信されたプログラムを実行して所定画像を生成し、生成された所定画像を表示するようにしたので、ユーザは、表示された画像を認証キーとして利用することができる。

【０２３８】また本発明の情報認証装置および方法、並びに第３のプログラムにおいては、第１の画像を撮像し、撮像された第１の画像に対応する第１の情報を認識し、認識された第１の情報に含まれるユーザIDを基に、他の装置に記録されているユーザ情報を検索し、検索されたユーザ情報を基に、第２の画像を生成するためのプログラムを作成し、作成されたプログラムを実行して第２の画像を生成し、生成された第２の画像に対応する第２の情報と、認識された第１の情報を認証するようにしたので、高精度にユーザ認証することができる。

【０２３９】さらにまた本発明の認証システムによれば、情報提供装置が、情報処理装置から送信されてくるプログラムの発行要求を受けて、情報処理装置に対して、ユーザIDを発行し、発行されたユーザID、および発行要求の受信時刻を基に、乱数を発生し、発生された乱数、ユーザID、および受信時刻を基に、第１の画像を生成するための第１のプログラムを作成し、作成された第１のプログラムを情報処理装置に提供し、ユーザIDに対応付けて、乱数および受信時刻を記録し、情報処理装置が、情報提供装置に対して第１のプログラムの送信を要求し、情報提供装置から提供される第１のプログラムを受信し、受信された第１のプログラムを実行して第１の画像を生成し、生成された第１の画像を表示し、情報認証装置でが、情報処理装置に表示されている第１の画像を撮像し、撮像された第１の画像に対応する第１の情報を認識し、認識された第１の情報に含まれるユーザIDを基に、情報提供装置に記録されている乱数および受信時刻を検索し、検索された乱数および受信時刻を基に、第２の画像を生成するための第２のプログラムを作成し、作成された第２のプログラムを実行して第２の画像を生成し、生成された第２の画像に対応する第２の情報と、

認識された第１の情報を認証するようにしたので、プログラム自体をユーザ毎に変化させて、それを認証キーとして機能させることにより、高精度にユーザ認証することができる。

【図面の簡単な説明】

【図１】本発明を適用したチケットレスシステムの一実施の形態の構成例を示す図である。

【図２】登録ユーザ情報データベースに記録されているユーザ情報の記録例を示す図である。

【図３】携帯電話機の外観の構成例を示す図である。

【図４】携帯電話機の表示部の外観の構成例を示す図である。

【図５】携帯電話機の内部の構成例を示すブロック図である。

【図６】携帯電話機の機能を説明するブロック図である。

【図７】チケットレス端末の外観の構成例を示す斜視図である。

【図８】図７のチケットレス端末の表示部を閉じた状態の構成を示す左側面図である。

【図９】図７のチケットレス端末の表示部を閉じた状態の構成を示す背面図である。

【図１０】チケットレス端末の内部の構成例を示す図である。

【図１１】チケットレス端末の機能を説明するブロック図である。

【図１２】サイバーコード生成プログラム発行／認証サーバの内部の構成例を示す図である。

【図１３】サイバーコード生成プログラム発行／認証サーバの機能を説明するブロック図である。

【図１４】サイバーコードを説明する図である。

【図１５】サイバーコード生成プログラムのダウンロード処理を説明するフローチャートである。

【図１６】携帯電話機の液晶ディスプレイに表示されるメニュー画面を示す図である。

【図１７】携帯電話機の液晶ディスプレイに表示されるダウンロード画面を示す図である。

【図１８】携帯電話機の液晶ディスプレイに表示されるサイバーチケットダウンロード画面を示す図である。

【図１９】携帯電話機の液晶ディスプレイに表示されるユーザ登録画面を示す図である。

【図２０】サイバーコードの認証処理を説明するフローチャートである。

【図２１】携帯電話機の液晶ディスプレイに表示されるJava（登録商標）アプレット実行画面を示す図である。

【図２２】携帯電話機の液晶ディスプレイに表示されるサイバーコードを示す図である。

【図２３】生成されるサイバーコードが変化する様子を説明する図である。

【図２４】サイバーコードファインダ起動時に表示される画面を示す図である。

【図２５】サイバーコード認証中に表示される画面を示す図である。

【図２６】サイバーコードが認識された場合に表示される画面を示す図である。

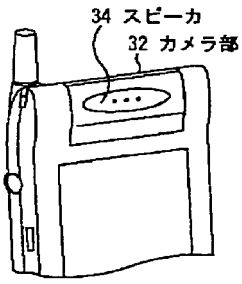
【図２７】ユーザIDの埋め込み方法を説明する図である。

【符号の説明】

１　カメラ付デジタル携帯電話機，　３　チケットレス端末，　７　インターネット，　８　サイバーコード認証サイト，　１１　サイバーコード生成プログラム発行／認証サーバ，　１２　登録ユーザ情報データベース，　３５　液晶ディスプレイ，　８２　ウェブブラウザ，　８３　表示プログラム，　８５　Java（登録商標）アプレット実行プログラム，　１０７　CCDカメラ，　１０９　液晶ディスプレイ，　１９２　サイバーコードファインダ，　１９３　認証プログラム，　２２２　Seed作成プログラム，　２２３　サイバーコード生成プログラム発行部，　２２４　認証用キー分離プログラム，　２２５　認証プログラム，２４１，２４２　サイバーコード

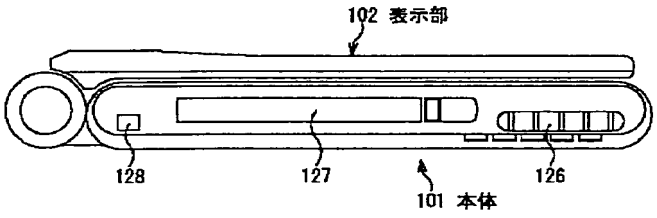
【図４】

図4

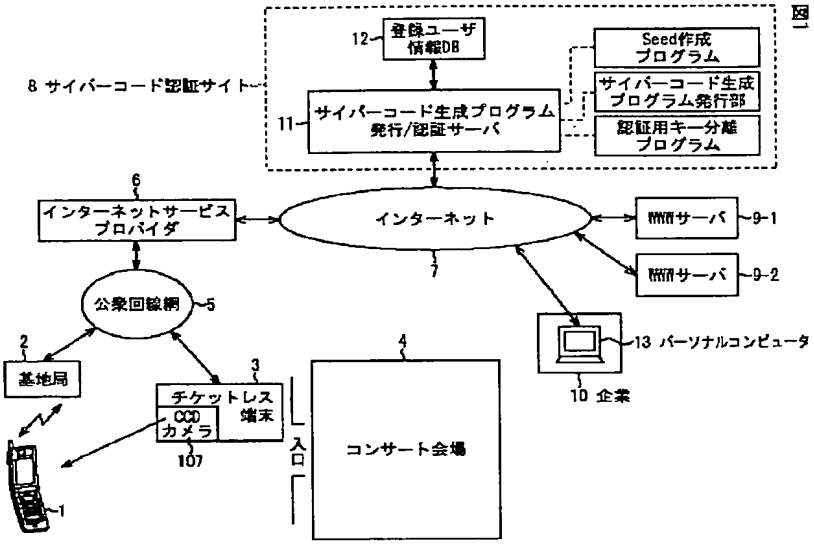


【図８】

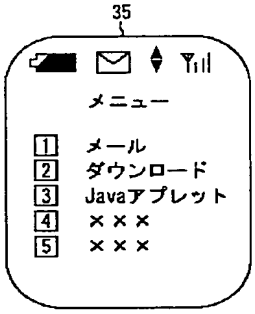
図8



【図１】



【図１６】

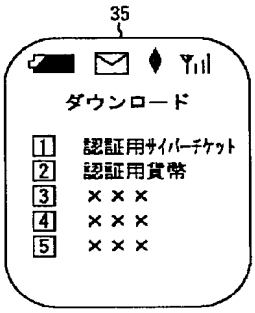


【図２】

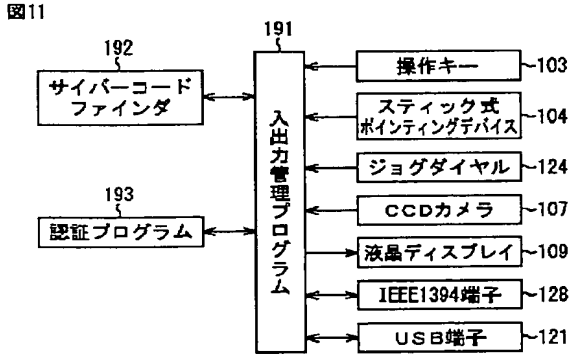
図2　図17

氏名	ユーザID	発行開始時刻	乱数発生用Seed	ユーザ情報
山田○○○	U_{001}	T_{001}	$Seed_{001}$	
田中△△△	U_{002}	T_{002}	$Seed_{002}$	
鈴木×××	U_{003}	T_{003}	$Seed_{003}$	

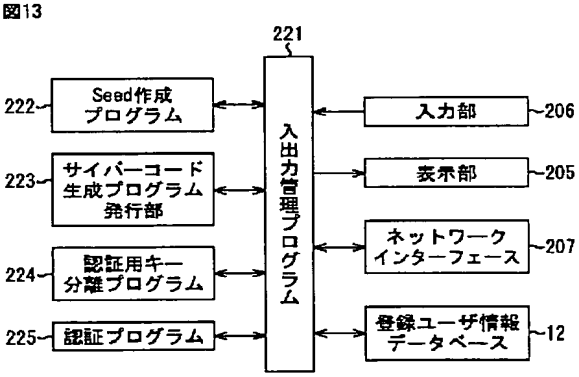
【図１７】



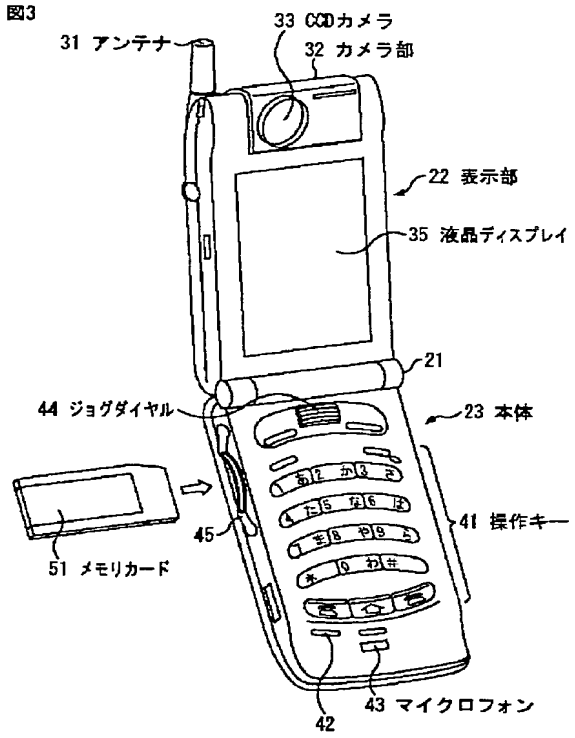
【図１１】



【図１３】

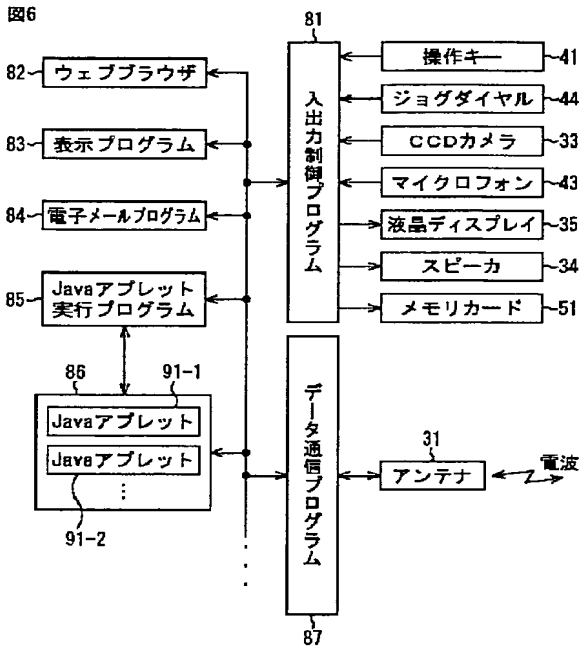


【図３】

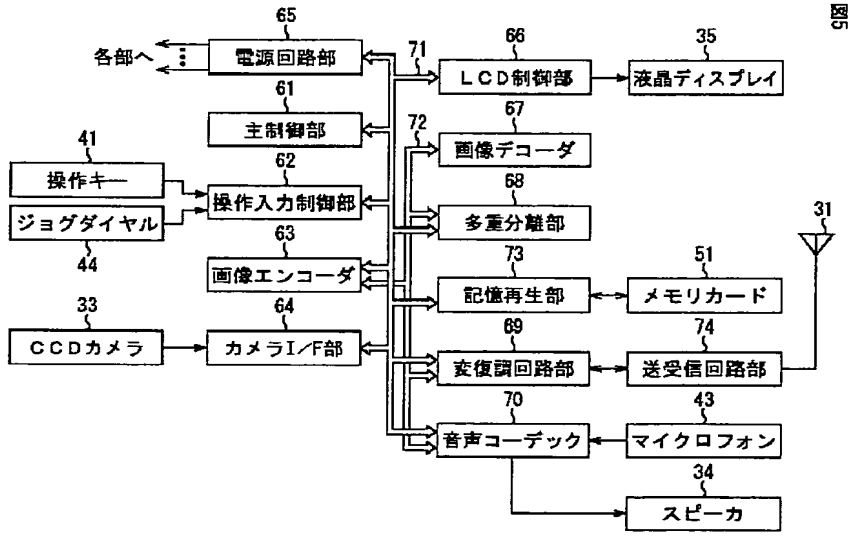


カメラ付デジタル携帯電話機 1

【図６】

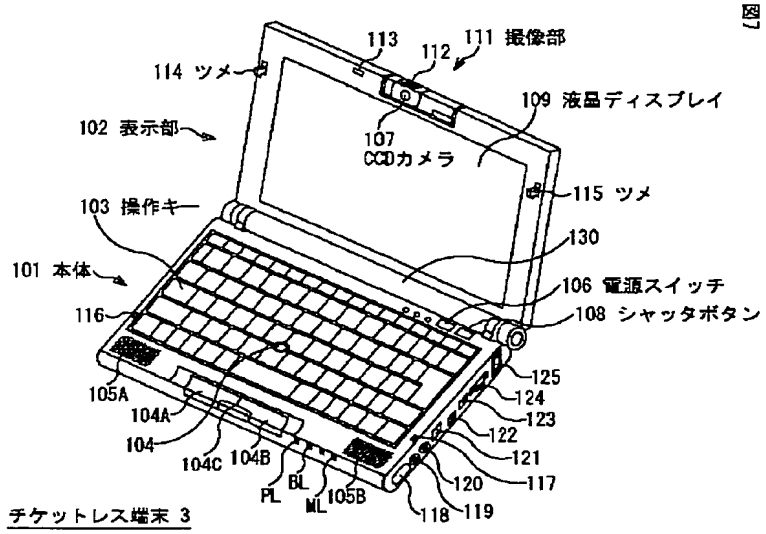


【図５】



【図７】

図7



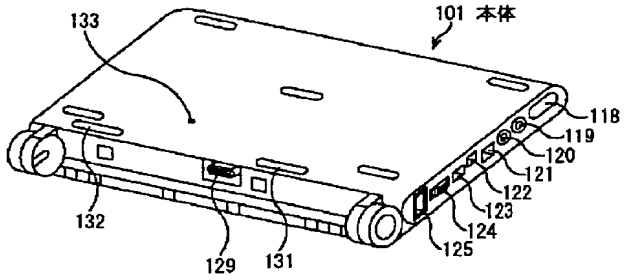
チケットレス端末 3

【図１８】

図18

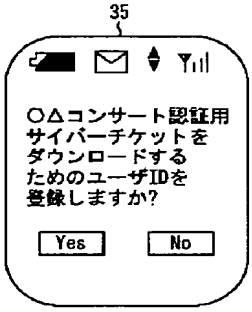
【図９】

図9



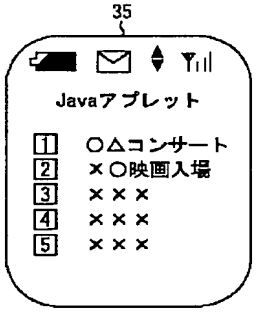
【図１９】

図19



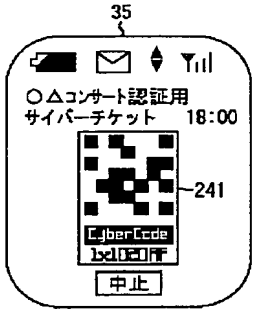
【図２１】

図21

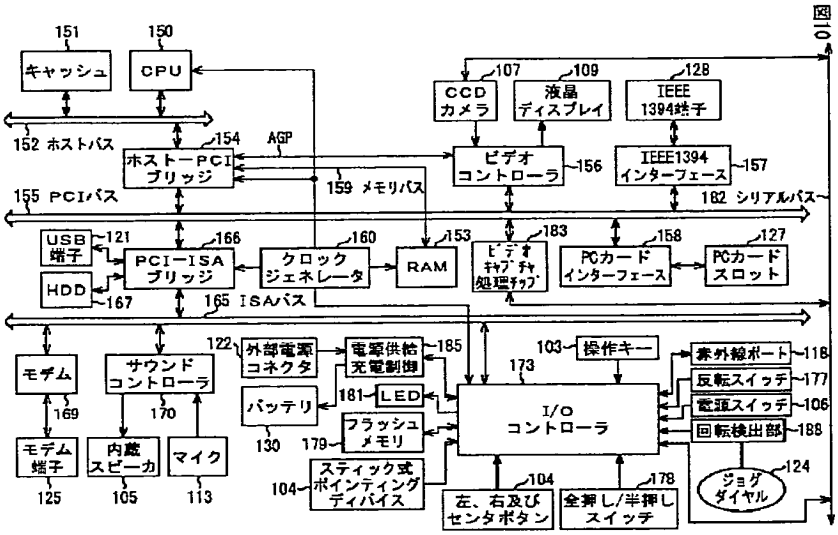


【図２２】

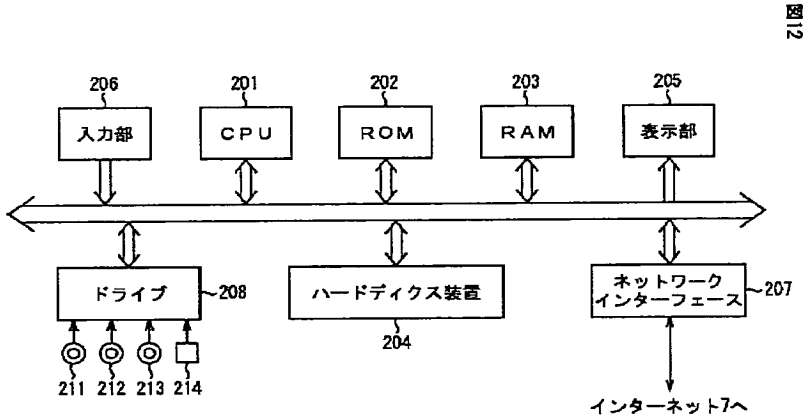
図22



【図１０】



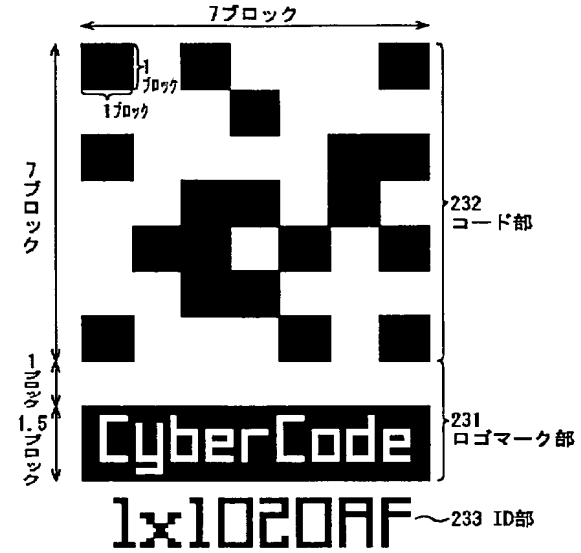
【図１２】



サイバーコード生成プログラム発行/認証サーバ 11

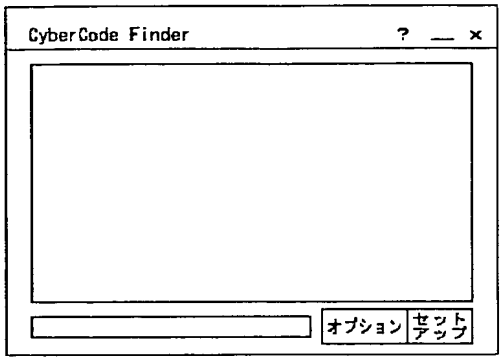
【図１４】

図14



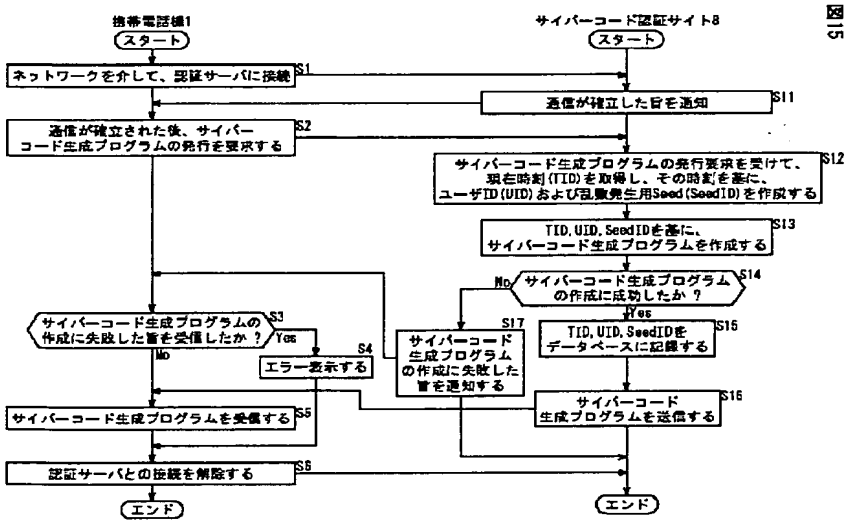
【図２４】

図24



【図１５】

図15



【図２０】

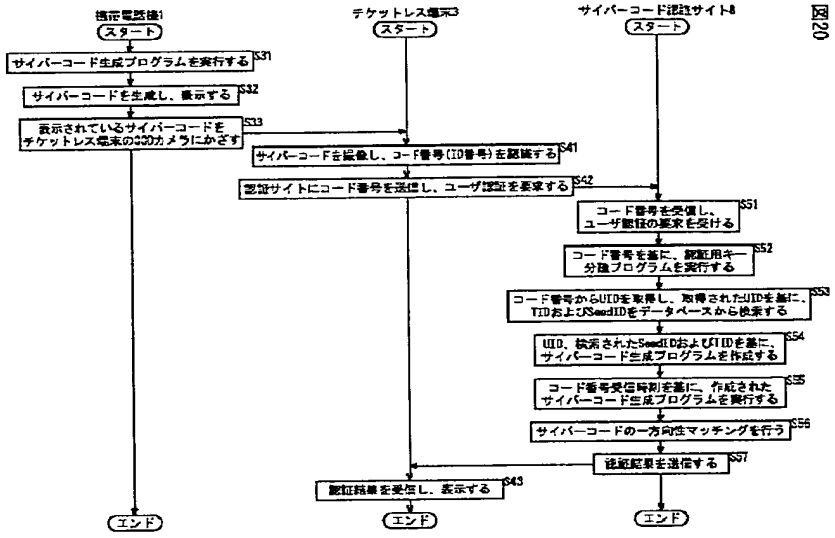
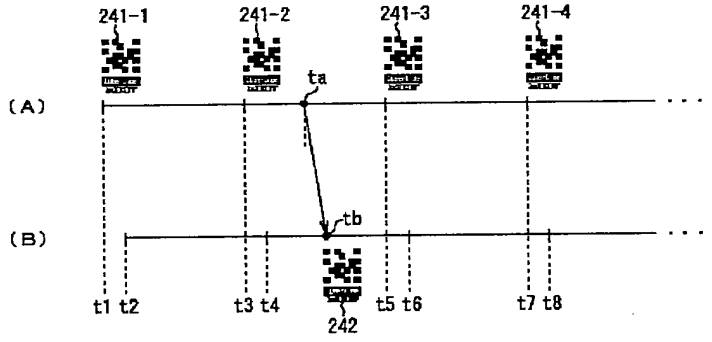


図20

【図２３】

図23



【図２５】

【図２６】

図25

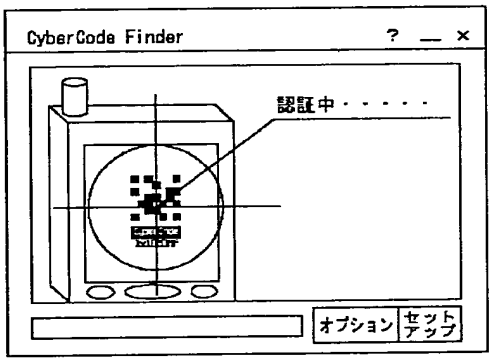
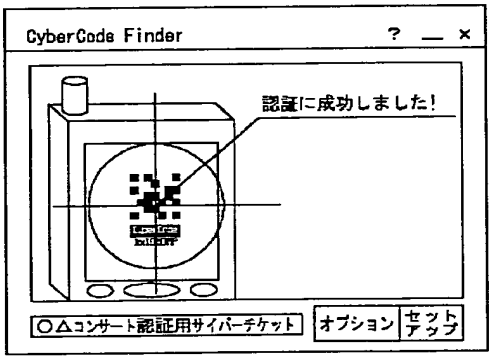
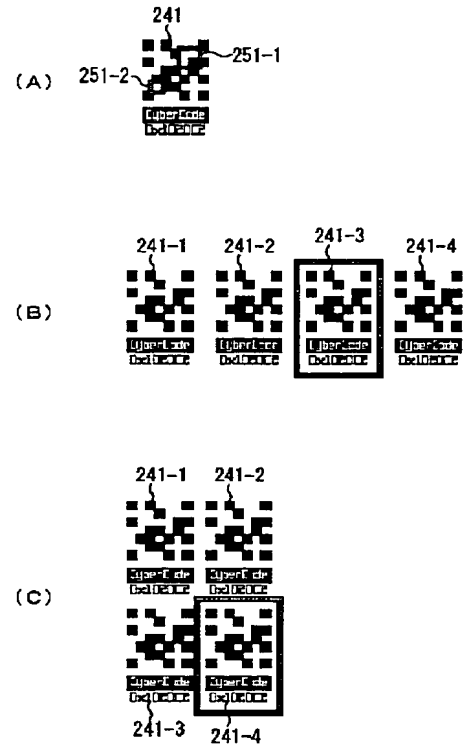


図26



【図２７】

図27



フロントページの続き

(51) Int. Cl.⁷	識別記号	F I	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０６Ｆ　17/60	５０６	Ｈ０４Ｌ　9/00	６７５Ｄ
			６７３Ｃ

(72)発明者　末吉　隆彦
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　綾塚　祐二
東京都品川区東五反田３丁目14番13号　株式会社ソニーコンピュータサイエンス研究所内
(72)発明者　松下　伸行
東京都品川区東五反田３丁目14番13号　株式会社ソニーコンピュータサイエンス研究所内
(72)発明者　暦本　純一
東京都品川区東五反田３丁目14番13号　株式会社ソニーコンピュータサイエンス研究所内

Ｆターム(参考)　5B017 AA06 BA07 BB09 BB10 CA15
5B085 AE01 AE08 BA07 BG07
5J104 AA07 BA07 GA03 GA05 KA01
KA04 MA01 NA04 NA35 NA41
NA43 PA02 PA10 PA11

THIS PAGE LEFT BLANK